

One law to rule them all? Strengthening global legal certainty for transborder flows of personal data

Doctoral Thesis

Philipp E. Fischer
Barcelona, July 2023

Universitat Oberta
de Catalunya



One law to rule them all? Strengthening global legal certainty for transborder flows of personal data

Doctoral Thesis to obtain the
International Doctorate Degree

Submitted by
Philipp E. Fischer

Doctoral Program on Information and Knowledge Society
Universitat Oberta de Catalunya

Thesis supervisor:
Dr. Miquel Peguera Poch

Thesis supervising committee:
Dr. Miquel Peguera Poch
Dr. Antoni Roig Batalla
Dr. Ricard Martínez Martínez

Barcelona, July 2023

Dedication

Für meine Seele

“If you’re walking down the right path
and you’re willing to keep walking,
eventually you’ll make progress.”

- Barack Obama -

TABLE OF CONTENTS

PREFACE AND ACKNOWLEDGEMENTS	10
INTRODUCTORY PART	11
CHAPTER I: FOUNDATIONS OF THE THESIS	12
I. The dimensions of transborder flows of personal data	12
1. Technological dimension	12
2. Economical dimension	18
3. Sociological dimension	25
4. Political dimension	30
II. Research questions, method, and scope	36
1. State of the question	36
2. Research questions and hypothesis	39
3. Research objectives	40
4. Methodological approach and workflow	41
4.1. International and comparative law	43
4.2. Cross-disciplinary and functional approach	45
4.3. General proposition-making and specific proposition-making methodologies	47
4.4. Smart Regulation and Better Regulation approaches	48
5. Scoping terminologies	50
5.1. Personal Data	51
5.2. Data Processing	53
5.3. Transborder flow	54
5.4. Privacy and Data Protection	55
5.5. Regulation	58
5.6. Jurisdiction	62
III. Conclusive remarks	64
FIRST PART: THE CURRENT WORLDWIDE REGULATORY MOSAIC	67
CHAPTER II: EUROPEAN FRAMEWORK	68
I. Legislative bodies and their relationships	68
II. Legislation of the EU	70
1. Union law system	70
2. Primary law regarding data protection	72
2.1. Art. 16 TFEU	72
2.2. Art. 39 TEU	73
2.3. Arts. 7 and 8 of the Charter	73
2.4. Internal and external perspectives: Arts. 51, 52, 53 of the Charter in relation with Art. 6 TEU	77
3. Secondary law regarding data protection	78
3.1. Directive 95/46	79

3.2.	E-Commerce Directive	84
3.3.	E-Privacy Directive / E-Privacy Regulation	86
3.4.	General Data Protection Regulation	90
3.4.1.	Subject-matter and objectives	90
3.4.2.	Scope	91
3.4.3.	Principles	93
3.4.4.	International data transfers	93
a.	Art. 44 GDPR (general principles for transfers)	95
b.	Art. 48 GDPR (transfers or disclosures not authorized by Union law)	99
c.	Art. 45 GDPR (transfers on the basis of an adequacy decision)	99
d.	Art. 46(1) GDPR (principle of prohibition for transfers)	101
e.	Art. 46(2) (a) GDPR (legally binding and enforceable instrument between public authorities or bodies as appropriate safeguard)	102
f.	Art. 46(2)(b) GDPR (BCR as appropriate safeguard)	103
g.	Art. 46(2)(c) GDPR (SDPC adopted by the Commission as appropriate safeguard)	104
h.	Art. 46(2)(d) GDPR (SDPC adopted by a SA and approved by the Commission as appropriate safeguard)	121
i.	Art. 46(2)(e) GDPR (CoC as appropriate safeguard)	122
j.	Art. 46(2)(f) GDPR (certification mechanism as appropriate safeguard)	122
k.	Art. 46(3) GDPR (ad-hoc clauses approved by a SA as appropriate safeguards)	123
l.	Art. 49 GDPR (derogations for specific situations)	124
3.5.	Law Enforcement Directive	132
3.6.	Passenger Name Record and Advance Passenger Information Directives	134
3.7.	E-Evidence package	139
3.8.	Digital Single Market Strategy and Data Strategy	150
3.8.1.	Digital Single Market Strategy and Free Flow of Data Initiative	150
3.8.2.	Data Strategy	151
4.	EU agreements with third countries or international organizations	159
4.1.	SWIFT Agreements	161
4.2.	PNR Agreements	162
4.3.	TTIP & CETA Agreements	165
4.4.	Umbrella Agreement	166
4.5.	Horizontal provisions	170
III.	Legislation of the Council of Europe	171
1.	European Convention on Human Rights	171
2.	Convention on Cyber Crime	175
3.	Convention 108 / Convention 108+	177
CHAPTER III: US FRAMEWORK		184
I.	Jurisprudence and variations of the right to privacy	184
II.	Regulatory instruments	188
1.	Federal legislation	188
1.1.	Pre-9/11 instruments	189
1.1.1.	Privacy Act	189
1.1.2.	Executive Order 12333	190
1.1.3.	Children's Online Privacy Protection Act	192
1.1.4.	Gramm-Leach-Bliley Act	193
1.1.5.	Internal Revenue Service Rule	194
1.2.	Post-9/11 instruments	194

1.2.1. Patriot Act / Freedom Act	195
1.2.2. Tracing Terrorist Financing Program	199
1.2.3. National Security Letters	201
1.2.4. FISA Amendments Act	202
1.2.5. Presidential Policy Directive 28 and Executive Order 14086	207
1.2.6. Judicial Redress Act	209
1.2.7. Cloud Act	211
1.2.8. Initiatives for a Federal Data Protection Law	215
2. Selected State legislation	222
III. The role of the Federal Trade Commission	230
 CHAPTER IV: ASIA-PACIFIC FRAMEWORK	233
I. Asia-Pacific Economic Cooperation (APEC)	234
1. APEC Privacy Framework 2005	234
2. APEC Data Privacy Pathfinder and CPEA	235
3. APEC Cross Border Privacy Rules	236
4. APEC Privacy Framework 2015	238
II. ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN)	239
1. ASEAN Framework on Personal Data Protection	239
2. ASEAN Framework on Digital Data Governance	239
III. Trans-Pacific Partnership and others	241
IV. China	243
1. Constitution	244
2. Cybersecurity Law	244
3. Civil Code	248
4. Data Security Law	248
5. Personal Information Protection Law (PIPL)	249
 CHAPTER V: INTERNATIONAL ORGANIZATIONS FRAMEWORK	257
I. OECD	258
1. Guidelines 1980	258
2. Guidelines 2013	260
3. Global Privacy Enforcement Network	261
II. United Nations	261
1. Universal Declaration of Human Rights	262
2. International Bill of Human Rights	263
3. Guidelines for the Regulation of Computerized Personal Data Files	267
4. Resolution on the right to privacy in the digital age, and others within the UN system	268
III. World Trade Organization	270
 CHAPTER VI: SELF-REGULATION	277
I. Pure self-regulation	278
1. Guidelines	278
2. Privacy Enhancing Technologies	280
II. Co-regulation	281
1. Guidelines	281
2. Privacy Enhancing Technologies	282
 CHAPTER VII: CONCLUSIVE REMARKS ON THE REGULATORY MOSAIC	283
 SECOND PART: THE PATH TO OVERCOME THE REGULATORY MOSAIC	286

CHAPTER VIII: PROBLEM CATEGORIES AND PROBLEM DRIVERS	287
I. The dilemma of a free flow of data vs. data flow restrictions	288
1. National digital economy	292
2. National security and national public order	301
3. Adequacy and gaps in coverage	306
II. Different approaches to the nature and scope of the right to data protection	310
III. Extraterritoriality and blocking statutes	318
IV. Conclusive remarks	327
 CHAPTER IX: THE GLOBAL ECOSYSTEM OF TRANSBORDER FLOWS OF PERSONAL DATA	 333
I. Endogenous variables	336
1. Stakeholders of a transborder flow of personal data flow scenario	338
1.1. Data controllers	338
1.2. Data (sub-)processors	346
1.3. Data subjects	346
1.4. Supervisory Authorities and Data Protection Officers	349
2. Stakeholders of a regulatory process	352
2.1. National and supranational level	353
2.2. International level	361
II. Arenas	364
1. EU-US	364
2. US	369
3. EU	371
III. Exogenous variables	383
1. Framework archetypes	384
1.1. Objective	385
1.2. Default position	390
1.3. Legal force and jurisdictional reach	391
1.4. Universal vs. limited approach to data governance	393
1.4.1. Transfer mechanisms	394
1.4.2. Regulatory cooperation	402
1.4.3. Technical standards	402
1.4.4. International trade rules	402
1.5. Maturity	403
2. Data protection principles	414
3. Essential guarantees	419
IV. Conclusive remarks	436
 CHAPTER X: OBJECTIVES FOR INTERVENTION	 441
I. General objective	442
II. Specific objectives	445
1. Consensus	445
2. Universality	447
3. Human-centricity	455
4. Maturity	459
5. Trust	460
6. Cooperation	463
7. Innovation	466
III. Conflict of objectives	471
IV. Conclusive remarks	473

CHAPTER XI: OPTIONS FOR INTERVENTION	478
I. No action	479
II. Non-legislative action	481
III. Legislative action	482
1. Improvement of existing regulation	483
1.1. National / supranational law	483
1.2. International law	489
2. Enactment of new regulation	493
IV. Conclusive remarks	495
 CHAPTER XII: OPERATIONALIZING THE PREFERRED INTERVENTION OPTION	 497
I. Basics: Building international uniform law	497
II. Process: UN law-making	501
III. Instrument: Improved Convention 108+ ruleset	505
1. Legislative elements	505
2. Non-legislative elements	520
IV. Competent authorities: UN Human Rights Council, International Court of Justice for Cyberspace Affairs	523
V. Conclusive remarks	525
 CONCLUSIONS	 527
 EPILOG	 537
 ABBREVIATIONS AND ACRONYMS	 546
 BIBLIOGRAPHY	 556

Note:

The research for this thesis was completed on 30 June 2023. Subsequent developments in the relevant law are therefore not reflected in this thesis unless otherwise stated.

PREFACE AND ACKNOWLEDGEMENTS

First, I would like to thank the supervising committee, Professor Miquel Peguera Poch, Professor Antoni Roig Batalla, and Professor Ricard Martínez Martínez for helping me complete this research.

My supervisor Miquel has not just been a valued “*Doktorvater*”. His leadership, generosity and constructive guidance have been a true inspiration for me. Coming from a German legal background, it was an extraordinary positive surprise, to which outstanding extent – in comparison to some modes of conducting a doctoral thesis at German Chairs of Law – Miquel was constantly involved in the progress. Miquel has been a source of strength to me not losing sight of my long-held goal of completing this thesis despite my not continuously possible portion of availability at the highest level due to two fatherhoods, full-time employment in parallel or in between phases of investing in the evolution of this thesis, and more.

I would also like to express my gratitude to the Max Planck Institute for Innovation and Competition in Munich, which provided me with wonderful resources. I have been squatting there over the years and it has become my second academic home. I would like to thank Professor Josef Drexl and Doctor Eva-Marina Bastian. They have been very lenient with me since I had to stretch my stay in various capacities (i.e., scholarship holder, researcher with a contract, guest). This enabled me in particular over the past two years to push this work through in one and more sustainable go and hereby to assure me also the international doctor mention.

My gratitude also goes to Professor Julia Hörnle. I dearly remember the meeting in 2010 in her office at the Centre for Commercial Law Studies at Queen Mary University of London, when she told me over a good English cup of tea that my research interest at that time – “Will Privacy Law in the 21st Century be American, European or International?” – was not actually a LL.M. thesis in terms of scope, but should be turned into a doctoral thesis. She got the ball rolling.

Personally, I would also like to thank my friends who have supported me during these many years, encouraged me to carry on, and to keep my motivation and persistence, which is anchored in me, always awake at the right time. A special thank you goes therefore to Doctor Marc Dominic Mimler and Doctor Stefan Zwerenz.

Finally, I would like to thank my family for their everlasting and unshaking backing to get this work done. This thesis would have not been possible without the endless loving help of them. My boys, not yet born when I started this work, have now, aged 4 and 7, seem to have become indulgent with me and realized the importance their father placed for years on something what my children still consider “Papa’s boring book”. My next literary achievement shall therefore be a reading book for children.

INTRODUCTORY PART

Rapidly developing technologies are providing new and powerful means to process data¹. The development of the Internet has made it possible to transfer these data “around the globe at the click of a mouse”². “Transborder flows of personal data” (TFPD) affect various “dimensions” in today’s society, including that of the law. Our investigative process in this interdisciplinary environment starts in Chapter I Section I presenting those relevant dimensions or forces at play, which in sum signify the relevance of TFPD for technology, economy, sociology, and policy; and on the other hand the impact of those four dimensions on TFPD.

Chapter I, Section II deals with the state of the question, the five research questions and the research objectives. A larger part is devoted to the description of the methodological approach. This is because the progress of this thesis is an interdisciplinary one and special attention must be paid to determining the workflow already at the beginning of the thesis. The dimensions to be described in Chapter I Section I. also make the scoping of the thesis relevant. It must be dealt with six “scoping terminologies” in Chapter I Section II more extensively than in scientific contributions to other areas of law. However, these terminologies are not conclusive, but in our opinion among the most important for the scoping of this thesis. Other terms will be determined during the FIRST PART. In Chapter I Section II, only general definitions from a global perspective are carried out, whilst the question of how different national, regional, or international regulations use this terminology will be described below in the FIRST PART.

¹ “Data” is understood in the plural in this thesis, although some quotes may use “data” in the singular

² Kuner, C. [Christopher]. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25 (4), 307–317. P. 308.

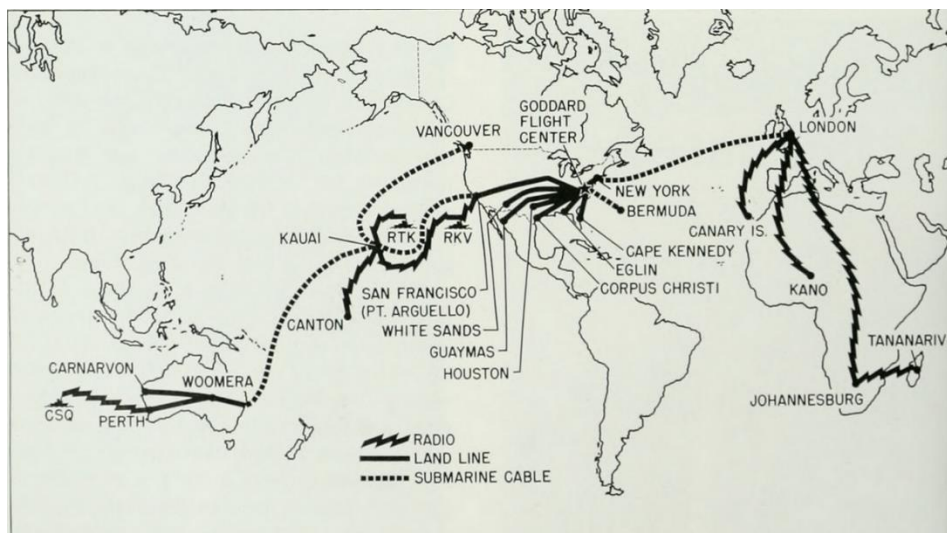
CHAPTER I: FOUNDATIONS OF THE THESIS

I. The dimensions of transborder flows of personal data

Aligned with the approach of Gasser³, this Section I wants to offer observations on TFPD from cross-jurisdictional perspectives. It shall include “forces at play” as real-world examples or “phenomena” within the field of data protection to make the global dynamism of the topic more understandable. It shall also highlight how the complex interplay among technical, economic, sociological, political, and, ultimately, normative forces threaten the consumer’s data protection space. Such “forces”, which then lead to “changes”, shall be divided into four different “dimensions”: 1) Technology, 2) Economics, 3) Sociology and 4) Politics. This Section I shall offer only perspectives rather than a comprehensive analysis of all possible drivers of the problem, which will be left to Chapter VIII.

1. Technological dimension

The dimensions to be explained in this Chapter I, Section I have not always been closely linked. In view of the matter of course today, with which the economic potential of the Internet is regularly emphasized, the fact that the establishment of cyberspace originally had no economic implications, may be surprising. From a technological perspective, “flows of data” beyond national borders have always existed. After the first transatlantic cables in the 1850s and the first transatlantic telephone cable in the 1950s, messages were transmitted, telegrams sent, telephone calls made.



Source: Akerman, N. [Nick], “Image from page 359 of Bell telephone magazine (1922)”⁴

³ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015 (2), 339–448. P. 355–374. The methodology is dealt with in more detail in Chapter I, Section II.4.

⁴ Medium Corporation. (2018, 3 December). Extraterritorial application of the GDPR [blog post]. *Golden Data Law*. <https://medium.com/golden-data/extraterritorial-application-of-the-gdpr-fff3dfbb8c4>.

The modern age of communication only began with the Internet, whose beginnings trace back to the 1950s. In 1958, the “United States (US) Department of Defense” founded the “Advanced Research Projects Agency” (ARPA), which was subsequently funded by the “National Science Foundation” (NSF), and whose task was, among other things, to develop communication systems to guarantee nationwide data transfer even if one part of the system failed.⁵ In the initial phase of the development of the Internet, only universities and a number of governmental and private research institutions were included. The first physical connection for transborder data flows was established in 1990 when the “European Organization for Nuclear Research” (CERN) connected to the US-based Cornell University with a 1.5 Mbit/s (T-1) transatlantic link.⁶ The private use of the Internet, which was previously excluded according to the “Acceptable Use Policy” (AUP)⁷ of the NSF, can be dated back to 1992-1993. It was then when “Mosaic”, “the first freely available Web browser to allow Web pages to include both graphics and text, was developed by students and staff working at the NSF-supported National Center for Supercomputing Applications”.⁸ The proliferation of commercial firms noticing the chances of the new communication form “led to an NSF solicitation in 1993 that outlined a new Internet architecture that largely remains in place today”⁹. The “World Wide Web” (WWW) was born.

It was then that jurisprudence began to take a closer look at the Internet. The first interest concerned both the Internet as a communication medium and the processes of normative control related to it. Except for the US, which had a significant impact from the beginning because of its financial support granted in the early development phase, the organization and development of behavioral guidelines on the Internet took place only by self-control processes of universities, administrative agencies, and research institutions. Due to the small number and extensive homogeneity of interests of the stakeholders involved and the low level of awareness of this medium, the absence of specific sovereign regulations was not considered a problem. Only the opening of the Internet to the private sector starting in the 1990s sparked a debate about the commercialization of the Internet and the necessity of elaborating legal structures.¹⁰ In the course of this discussion, the positive experiences with self-regulation structures, particularly in the form of so-called “netiquettes” in the early social media use, continued to have a formative effect. However, despite the enthusiasm that was brought up for the idea of a private “*lex informatica*”, the view changed quickly to that the Internet shall not represent a space beyond legal standardization.¹¹ A common understanding evolved that constructive coexistence of sovereign external control on the one hand and self-control mechanisms on the other hand is required.¹²

⁵ Waldrop, M. [Mitch]. (2015). DARPA and the Internet Revolution. *Defense Advanced Research Projects Agency, 2015*, 78-85. [https://www.darpa.mil/attachments/\(2015\)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20\(Approved\).pdf](https://www.darpa.mil/attachments/(2015)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf).

⁶ Segal, B. [Ben]. (1995). *A Short History of Internet Protocols at CERN*. <https://ben.web.cern.ch/ben/TCPHIST.html>.

⁷ AUP documents were written for corporations, businesses, universities, schools, ISPs, and website owners.

⁸ National Science Foundation. (2003). *A Brief History of NSF and the Internet*.

https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

⁹ National Science Foundation. (2003). *A Brief History of NSF and the Internet*.

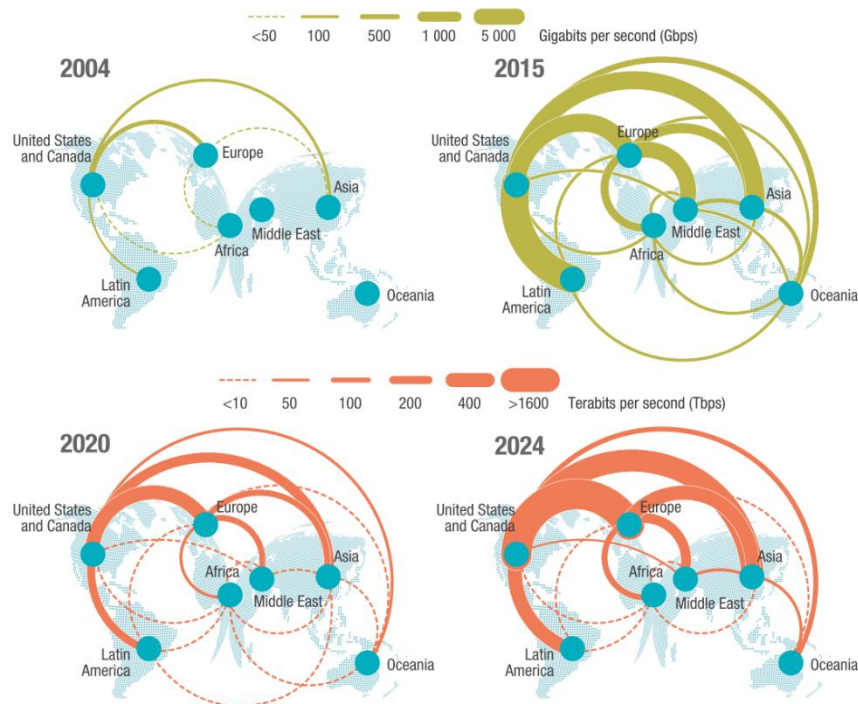
https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050

¹⁰ Engel, C. [Christoph]. (2000). Das Internet und der Nationalstaat. Völkerrecht und Internationales Privatrecht in einem sich globalisierenden internationalen System – Auswirkungen der Entstaatlichung transnationaler Rechtsbeziehungen. *Berichte der Deutschen Gesellschaft für Völkerrecht*, 39, 353–425. P. 368. // Zimmermann, S. [Stefan]. (2009). *E-Commerce, Verbraucherschutz und die Entwicklung Intelligenter Agenten*. Peter Lang. P. 18 ff.

¹¹ Reidenberg, J. [Joel]. (1996). Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*, 45, 911–930. P. 929–930.

¹² Röben, V. [Volker]. (1999). International Internet Governance. In J. [Jost] Delbrück and R. [Rainer] Hofmann, *German Yearbook of International Law - Jahrbuch für Internationales Recht.: Vol. 42 (1999)* (pp. 400-437). Duncker & Humblot. // Ibáñez, J. [Josep]. (2008). Who Governs the Internet? The Emerging Regime of E-Commerce. In A. [Andreas] Nölke and J.-C. [Jean-Christophe] Graz, *Transnational Private Governance and its Limits* (pp. 142–155). Routledge.

Internet nodes serve as exchange points for the data traffic of the Internet. Statistics on such nodes highlight the increase of the global Internet traffic in the last years. The world's largest "Commercial Internet Node" (CIX) is the "DE-CIX" in Frankfurt am Main, Germany. DE-CIX Frankfurt statistics annotate, based on a 5-year overall traffic graph, a doubling of the traffic exchanged at DE-CIX Frankfurt (13 terabytes per second by end-2022).¹³ The "United Nations Conference on Trade and Development" (UNCTAD) presented similar numbers:



Source: UNCTAD, "Evolution of interregional international bandwidth, selected years"¹⁴

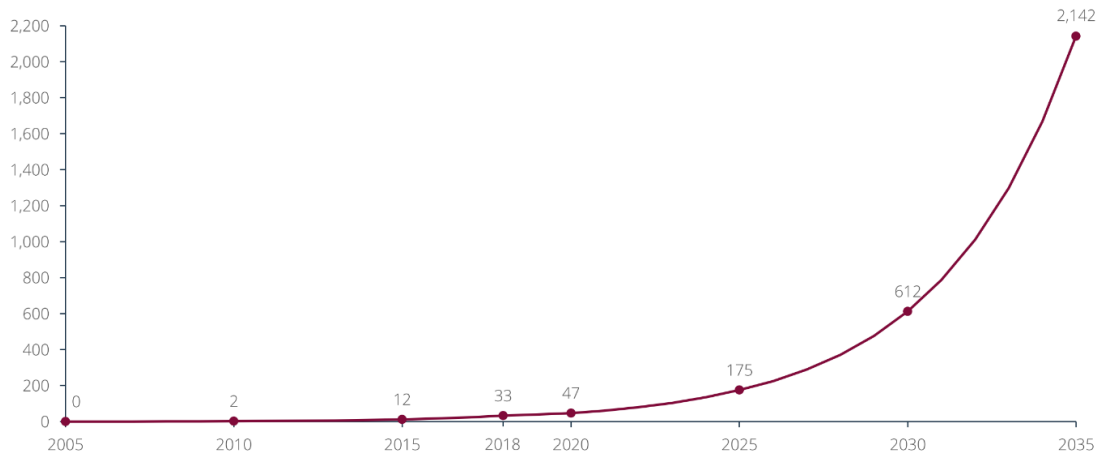
Cisco projected a 45x multiplication of traffic between 2005 and 2014.¹⁵ Seagate predicted that the amount of data produced worldwide increases rapidly, from 33 zettabytes in 2018 to an expected 160 zettabytes in 2025, which is equivalent to an almost fivefold multiplication.¹⁶ This trend will continue and increase the global amount of data created per year:

¹³ DE-CIX Management GmbH. (2022). *Traffic Frankfurt – 5 years*. <https://www.de-cix.net/en/locations/germany/frankfurt/statistics>

¹⁴ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 21.

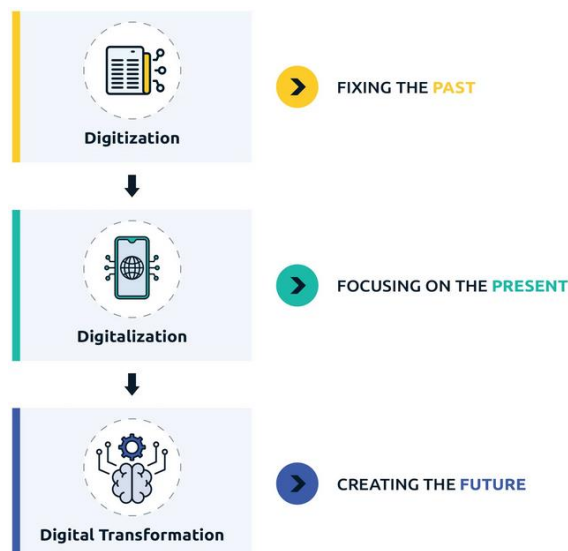
¹⁵ McKinsey Global Institute. (2016). *Digital globalization: The new era of global flows*. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>.

¹⁶ Reinsel, D. [David]. (2017). *Data Age 2025: The Evolution of Data to Life-Critical*. IDC White Paper. <https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>. P. 7.



Source: Statista, "Worldwide amount of data created per year in zettabytes"¹⁷

"Digitization", "digitalization", and "digital transformation" shape professional and private life of a large majority of citizens.¹⁸



Source: Dieffenbacher, S. F. [Stefan F.]. "Digitization vs Digitalization vs Digital Transformation"¹⁹

One scenario in this environment is the use of an "Internet Service Provider" (ISP)²⁰, which exchanges data between networks across the CIXs. Exemplarily for the US, the "Federal Trade Commission" (FTC) found that US-based ISPs

¹⁷ Buss, S. [Sebastian]. (2019). *Digital Economy Compass 2019*. Statista GmbH. <https://de.statista.com/statistik/studie/id/52312/dokument/digital-economy-compass/>. P. 6.

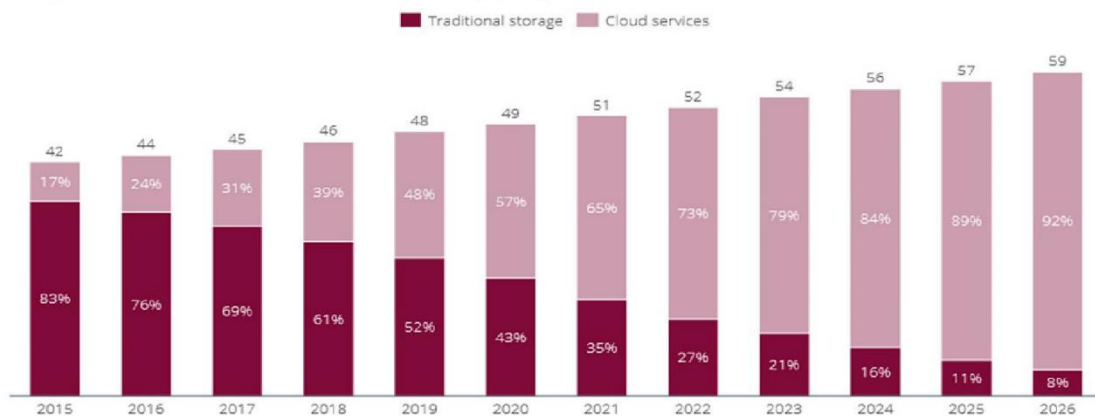
¹⁸ Looking at the English-speaking world, there is a meaningful distinction between "digitization" and "digitalization". Digitization refers to the phenomenon that information previously stored in analog form is now available digitally as zeros and ones. This development already began with the use of the first computers. Digitization is a prerequisite for "digitalization". The latter encompasses changes shaped by new, creative use of digital data, which can even lead to changes in user behavior and the transformation of entire business models. "Digital transformation" is business transformation enabled by digitalization.

¹⁹ Dieffenbacher, S. F. [Stefan F.]. (4 March 2023). *Digitization vs Digitalization: Differences, Definitions, and Examples*. <https://digitalleadership.com/blog/digitization-vs-digitalization>.

²⁰ A "Service Provider" (SP) is a business which provides services. In the context of the Digital Economy, a SP encompasses different types. An ISP provides internet services. A "Cloud Service Provider" (CSP) is a business that offers applications in the Cloud – typically "Infrastructure as a Service" (IaaS), "Software as a Service" (SaaS), or "Platform as a Service" (PaaS).

have evolved into technology giants who offer not just internet services but also provide a range of other services including voice, content, smart devices, advertising, and analytics – which has increased the volume of information they are capable of collecting about their customers. [They] collect and share far more data about their customers than many consumers may expect – including access to all of their Internet traffic and real-time location data – while failing to offer consumers meaningful choices about how this data can be used” and concluded that “ISPs’ data collection and use practices mirror problems identified in other industries and underscore the importance of restricting data collection and use.²¹

Another scenario is the use of a CSP. “Cloud Computing” concerns the shift of IT services to the WWW. This allows the deployment and use of IT infrastructures, platforms and applications in “the Cloud”. In these cases, a user can book a service with a CSP. The latter then operates the required hardware and, depending on the application model, operates the necessary software or services and makes them available to the user. Cloud Computing provides the user with high flexibility and scalability of IT resources, as the Cloud facilitates to acquire resources in the required quantity when they are needed. Personal data processed in by a CSP can be forwarded for processing to other data centers of the initially contracted CSP, or to another CSP. Cloud Computing has become a “driver to illustrate the speed and breadth of the environment”²², which also the following graphic showcases.



Source: Statista, “Worldwide revenues from enterprise storage in billion USD”²³

Schwartz referred to a “massive growth in the complexity and volume”²⁴ of “transborder flows of personal data” (TFPD), accompanied by a change in the nature of such transfers in that they, in fact, no longer constitute point-to-point transmissions, but “occur today as part of a networked series of processes made to deliver a business result”²⁵. In such an environment, scenarios of TFPD are the rule.

“Artificial Intelligence” (AI) changes areas of life across several use cases connected with the processing of personal data. Those are, e.g., Chatbots, digital assistants such as

²¹ Federal Trade Commission. (2021). *WFTC Staff Report Finds Many Internet Service Providers Collect Troves of Personal Data, Users Have Few Options to Restrict Use*. <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-staff-report-finds-many-internet-service-providers-collect-troves-personal-data-users-have-few>.

²² Robinson, N. [Neil]. (2009). Has European Data Protection Law Become Outdated? *Zeitschrift für Multimedia und Recht*, 2009 (11), 725–726. P. 726

²³ Buss, S. [Sebastian]. (2019). *Digital Economy Compass 2019*. Statista GmbH. <https://de.statista.com/statistik/studie/id/52312/dokument/digital-economy-compass>. P. 12.

²⁴ Schwartz, P. M. [Paul M.]. (2009). *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment*. *Privacy Projects*. https://paulschwartz.net/wp-content/uploads/2019/01/Global_Data_Flows.pdf. P. 4.

²⁵ Schwartz, P. M. [Paul M.]. (2009). *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment*. *Privacy Projects*. https://paulschwartz.net/wp-content/uploads/2019/01/Global_Data_Flows.pdf. P. 4.

“Alexa” (by Amazon), “Siri” (by Apple) and “Google Assistant” (by Google), intensified diagnosis procedures in the healthcare sector, and more cost-effective results through automated decision-making. Such use cases usually establish identifiability of individuals which opens the scope of application of regulations on data protection. Implementing requirements such as those of the “General Data Protection Regulation”²⁶ (GDPR) of the “European Union” (the Union or EU) – in particular those of the transparency principle and the rights of data subjects – with regard to the development and use of AI remained a challenge. SAs have, for example, raised data protection concerns regarding an AI-driven product from the US-group “Open AI”, but not on the underlying AI model, but on the AI training and the end-user product “ChatGPT”. The Italian SA issued a ban on use, basing this on the lack of sufficient transparency.²⁷ Open AI had used all data freely available on the Internet for the AI training. Insofar as this included personal data, the data subjects were not informed and there was no legal basis for the processing of personal data. Likewise, no information had been provided to end customers of ChatGPT. Furthermore, ChatGPT did not delete or correct incorrect results of this processing as required by the GDPR. The “European Commission” (the Commission) intended rules to protect health, safety and fundamental rights of persons affected by such AI use cases. To this end, it presented a proposal²⁸ for an EU regulatory framework on AI

to enact a horizontal regulation of AI. The proposed legal framework focuses on the specific utilization of AI systems and associated risks. The Commission proposes to establish a technology-neutral definition of AI systems in EU law and to lay down a classification for AI systems with different requirements and obligations tailored on a ‘risk-based approach’. Some AI systems presenting ‘unacceptable’ risks would be prohibited. A wide range of ‘high-risk’ AI systems would be authorized, but subject to a set of requirements and obligations to gain access to the EU market. Those AI systems presenting only ‘limited risk’ would be subject to very light transparency obligations.²⁹

More than a year after its introduction in April 2021, this proposed “AI Act” is still up for negotiation and debate.³⁰ Therefore, “the EU lost its first-mover advantage as other jurisdictions like China and Brazil have managed to pass their legislation first”³¹. The regulation of AI from a data protection perspective is not solely a phenomenon of the European framework, but concerns the global level, which is why considerations in this regard must be generalized.

The technological dimension has also a data infrastructure perspective. Ursula von der Leyen, President of the Commission, stated that while it may be too late to replicate “hyperscalers”, it is still time to achieve “technological sovereignty” in some key areas.³²

²⁶ European Commission. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, Official Journal of the European Union L 119 (4 May 2016), 1–88. (“GDPR”).

²⁷ Goujard, C. [Clothilde]. (31 March 2023). Italian privacy regulator bans ChatGPT. *Politico*. <https://www.politico.eu/article/italian-privacy-regulator-bans-chatgpt>.

²⁸ EU. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM(2021) 206 final, (21 April 2021).

²⁹ Madiaga, T. [Tambiana]. (January 2022). Artificial intelligence act. *European Parliamentary Research Service*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf). P. 2.

³⁰ The latest update in this development was the publication of the European Parliament’s negotiating position on the AI Act. // European Parliament. (14 June 2023). *MEPs ready to negotiate first-ever rules for safe and transparent AI*. <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>.

³¹ Bertuzzi, L. [Luca]. (9 February 2022). *Inside the EU's rocky path to regulate artificial intelligence*. <https://iapp.org/news/a/inside-the-eus-rocky-path-to-regulate-artificial-intelligence>.

³² von der Leyen, U. [Ursula]. (2019). *Union that strives for more. My agenda for Europe*. Publications Office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1>. P. 13–14.

Following this call, representatives of the German government, business and science, together with other European partners, aimed to create a next generation of a data infrastructure for Europe: a secure and networked data infrastructure that meets the highest standards of digital sovereignty and promotes innovation.³³ The project is intended to serve as the cradle of an open and transparent digital “ecosystem” in which data and services can be made available, brought together and shared in a trusting manner. This is to bring decentralized infrastructure services into a homogeneous, user-friendly system. With the help of this ecosystem, companies and business models from Europe should be able to scale competitively worldwide. This aims to ensure added value and employment in Europe by enhancing competitiveness with large US-based MNEs such as Google and Amazon.

This goal is also followed by the new “Data Strategy”³⁴ and the “Digital Compass 2030”³⁵ of the Commission. The latter wants to serve making progress in digitization in Europe measurable. It stipulates that every EU citizen should access its own medical files electronically and that all households in the EU should have Internet at gigabit speed. Further goals for the year 2030 are at least 80 percent of adults having basic digital skills, as well as 20 million computer specialists and at least 20 percent of the global production of semiconductors within the EU. The EU also wants a network of 10,000 climate-neutral data centers spread across the Union. Three out of four companies should use Clouds. Von der Leyen declared in her Agenda³⁶ digitization to be the top issue, especially since major deficiencies came to light in authorities, schools and companies during the pandemic. Now a “digital decade”³⁷ must follow, explained von der Leyen.

2. Economical dimension

The transformation within this technological dimension also affects the concept of global trade. The international flow of goods, services, and finance constantly increased at global level. Data flows represented in 2016 an estimated USD 2.8 trillion of this added value.³⁸ UNCTAD estimated in the same year that “about 50% of all traded services is enabled by innovation stemming from the technology sector including the facilitation of cross-border data flows”³⁹. Roger Wicker, Chairman of a US Senate’s hearing in December 2020, stated that

data is the lifeblood of the global digital economy. The free movement of data across national borders underpins trillions of dollars in international trade, commerce, and investment. Data serves as a catalyst for innovation, productivity, and economic growth, and helps promote U.S. competitiveness and technology leadership around the

³³ Altmaier, P. [Peter]. (2019). *Project GAIA-X*. Federal Ministry for Economic Affairs and Energy. https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=5. // See also Chapter II, Section II.3.8.2.

³⁴ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). (“Data Strategy”).

³⁵ European Commission. (9 March 2021). *Europe’s Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983.

³⁶ von der Leyen, U. [Ursula]. (2019). *Union that strives for more. My agenda for Europe*. Publications Office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1>. P. 13–14.

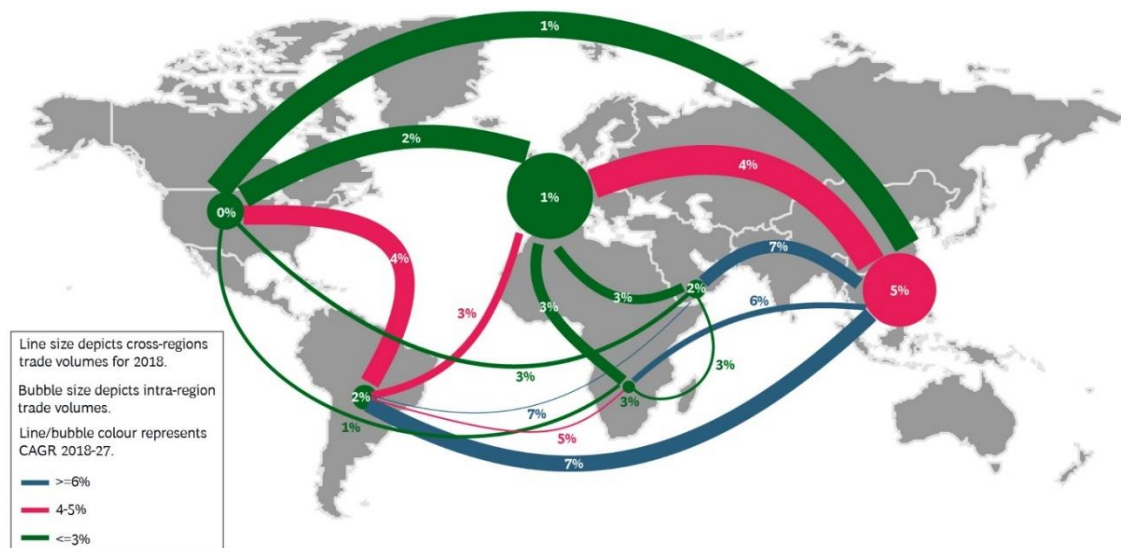
³⁷ von der Leyen, U. [Ursula]. [European Commission] (2 June 2021). *Message by President von der Leyen - “Leading the Digital Decade”*. YouTube. <https://www.youtube.com/watch?v=kpTDZMqkzxl>.

³⁸ Barayre, C. [Cécile]. (5 July 2016). *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. MIKTA Workshop on Electronic Commerce, Geneva, Switzerland. https://www.wto.org/english/forums_e/business_e/3_4_Cecile_ppt.pdf. P. 5.

³⁹ APEC. *Regulations, Policies and Initiatives on E-Commerce and digital economy for APEC MSMEs’ Participation in the Region*. https://www.apec.org/docs/default-source/publications/2020/3/regulations-policies-and-initiatives-on-e-commerce-and-digital-economy/220ecsgregulations-policies-and-initiatives-on-e-commerce-and-digital-economy-for-apec-msmes-particip.pdf?sfvrsn=63b748d7_1, (March 2020). P. 42.

world. [...] Digitally enabled trade amounted to between USD 800 and USD 1,500 billion globally in 2019 and is projected to raise global GDP by over USD 3 trillion in 2020.⁴⁰

Data flows between the US and Europe play an outstanding role in global trade. Those flows “are the largest in the world and are fundamental to the largest trading relationship in the world, valued at approximately 1.3 trillion U.S. dollars annually”.⁴¹ Trans-regional data flow relates to trans-regional trade flow. The global volume of trade nowadays runs essentially between EU countries, the countries of NAFTA (Canada, US and Mexico) as well as the countries of East and Southeast Asia (with China, Japan, South Korea and Singapore at the top), as the following graphic indicates:



Source: Patel, D. [Deepesh], “Global trade flows are expected to grow from 2018 to 2027, reaching USD 25T”⁴²

This trans-regional data flow not only concerns the exchange of data between contracting business Parties but also within the corporate structure of a MNE. Such enterprises “rely heavily on cross border data flows for their day-to-day operations: they use data from their affiliates around the world for a large number of internal, or back-office, tasks and even routine decisions. This includes moving human resources data to and from headquarters, sending data to R&D facilities located abroad, managing production processes and engaging in after-sale services.”⁴³ Due to the increasing networking of production and trade relationships, personal data may not only remain within a MNE but could also be transferred to foreign business partners as part of data outsourcing projects. These MNEs develop new business models by using personal data to provide customized services. While this might make life easier for end users, these services also entail a high-volume TFPD.

The economic use of the Internet is commonly discussed under the label of “Electronic Commerce” (E-Commerce). There is general agreement that only economically

⁴⁰ Wicker, R. [Roger]. (9 December 2020). *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows*. U.S. Senate Committee on Commerce, Science, and Transportation. <https://www.commerce.senate.gov/2020/12/the-invalidation-of-the-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows#>.

⁴¹ American Chamber of Commerce to the European Union. (30 July 2020). *Joint Industry Letter on Schrems II Case Ruling*. <https://www.itic.org/policy/JointIndustryLetterSchremsII-30July.pdf>. P. 1.

⁴² Patel, D. [Deepesh]. (2022). *Digital Ecosystems in Trade Finance: Seeing Beyond the Technology*. Trade Finance Global. <https://www.tradefinanceglobal.com/blockchain/digital-ecosystems-in-trade-finance>. // UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 19.

⁴³ Casalini, F. [Francesca]; López González, J. [Javier]. (2019). *Trade and cross-border data flows*. OECD Publishing. <https://doi.org/10.1787/b2023a47-en>. P. 14–15.

motivated trade and business activities that are carried out electronically are included in this definition, with the Internet today being the main technical infrastructure enabling these activities. Aaronson distinguished “between e-commerce (goods and services delivered via the internet and associated with a transaction) and digital trade, which includes e-commerce as well as new data-based services”⁴⁴. Nevertheless, business activities via telephone or fax, as well as electronic payments, are often included in the definition of E-Commerce. According to the “Organization for Economic Co-operation and Development” (OECD), this definition covers online orders, the offerings of market platforms such as Amazon or eBay, as well as the data uses of platforms such as Google or “Meta Platforms Inc.”⁴⁵ (Meta).⁴⁶

Global sales in E-Commerce increases constantly. It is forecasted that EUR 6.06 trillion in sales of physical goods in the B2C e-commerce market will be reached in 2027; this corresponds to an expected annual sales growth of 10.90% (CAGR 2023-2027); with a forecast market volume of EUR 1,451.00 billion in 2023, China will generate the most revenue; in the eCommerce market, the number of users is expected to reach 5.29 billion users in 2027; the penetration rate will be 57.2% in 2023 and is expected to reach 66.6% in 2027.⁴⁷

As early as 2017, a study of the Bavarian data protection authority on data transfers to non-EU countries with 150 audited companies in various sectors showcased the size of TFPD within E-Commerce.⁴⁸ This audit was commissioned as many German MNEs are headquartered in Bavaria and the Cloud is interesting for a large number of “Small and medium-sized enterprises” (SMEs) – including in Bavaria: 56% - Transfers to non-EU countries; thereof 33% - Transfers to the US and other non-EU countries; 13% - Transfers to the US, but not to other non-EU countries; 10% - Transfers not to the US, but to other non-EU countries.

An privacy governance report issued by the “International Association of Privacy Professionals” (IAPP) together with the consultancy firm EY found that more than 70% of 473 MNEs which operate at international level transfer personal data from the EU to a so-called “third country”⁴⁹.⁵⁰ Other data are provided by a survey conducted by Bitkom in September 2021, targeted at 502 companies with 20 or more employees in Germany.⁵¹ 52% reported that they transfer personal data to third countries. Out of these, personal data was transferred to the following countries: 52% US, 35% United Kingdom, 18% Russia, 13% India, 8% China, 7% Japan, 4% South Korea.

The number of unreported cases of transfers to countries outside the “European Economic Area” (EEA) and the EU is probably higher, as many companies are probably not always aware of the transfer to those destinations. Further, the companies indicated,

⁴⁴ Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 3.

⁴⁵ Meta Platforms Inc. is a US technology company that owns the social networks Facebook and Instagram, the instant messaging apps WhatsApp and Messenger, and Oculus, a creator of virtual reality technology.

⁴⁶ OECD. (2019). *Implications of E-commerce for Competition Policy - Background Note*. [https://one.oecd.org/document/DAF/COMP\(2018\)3/en/pdf](https://one.oecd.org/document/DAF/COMP(2018)3/en/pdf). P. 6.

⁴⁷ Statista GmbH. (2023). *Digital Market Insights eCommerce*. <https://de.statista.com/outlook/dmo/ecommerce/weltweit>

⁴⁸ Alexander, F. [Filip]. (2017). *Internationale Datentransfers - Sicht einer deutschen Aufsichtsbehörde*.

<https://docplayer.org/113788840-Internationale-datentransfers-sicht-einer-deutschen-aufsichtsbehoerde.html>.

⁴⁹ “Third country” in this thesis is not only understood from the perspective of Directive 95/46 or the GDPR but is always referred to as such when personal data is to be transferred to a non-member country of a specific regulatory instrument, thus outside the initial jurisdictional scope of that instrument.

⁵⁰ LaLonde, B. [Brandon] and Thompson, M. [Mark] and Kanthasamy, S. [Saz]. (2022). *IAPP-EY Annual Privacy Governance Report 2022 – Executive Summary*. <https://iapp.org/resources/article/privacy-governance-report/>. P. 4.

⁵¹ Bitkom. (15 September 2021). *Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers*. <https://www.bitkom.org/sites/default/files/2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf>.

among other things, that if they waived such transfers in 62% of the business cases, they could no longer offer certain products and services, in 57% they would run into competitive disadvantages compared to companies from non-EU countries, in 54% they would have higher costs, and in 4% global security support could not be maintained. The OECD has similarly underscored the importance of data flows in a competitive E-Commerce by noting that

data flows allow SMEs to access IT services, such as cloud computing, reducing the need for costly upfront investment in digital infrastructure. This allows them to be nimbler, quickly scaling-up IT functions in response to changes in demand. Better and faster access to critical knowledge and information also helps SMEs overcome informational disadvantages, notably with respect to larger firms, reducing barriers to engaging in international trade and allowing them more readily to compete with larger firms. [...]. Data is therefore a means for widening consumer choice and the affordability of goods and services, helping SMEs reach global markets and a key element of international production through GVCs [Global Value Chain].⁵²

Big Data has become another driver for the digital economy, affecting both providers and users. Business consultants Gartner Inc. defined Big Data as “high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making”⁵³. This definition points out the three most outlined dimensions of Big Data (known as the “3 Vs” which define Big Data): volume, velocity and variety:

- Volume: Huge amounts of data in the scale of zettabytes 4 and more.
- Velocity: Real time streams of data flowing from diverse resources (e.g. physical sensors or “virtual sensors” from social media, such as Twitter streams).
- Variety: Data from a vast range of systems and sensors, in different formats and datatypes.

At its core, Big Data is about analytically linking the ever-increasing amounts of data to gain economic, social or scientific insights. The size of so-called “datasets”⁵⁴ used hereby is only one aspect of the phenomenon, as quantitative and qualitative characteristics are intertwined. The sheer amount of information can help to compensate for the lower quality in small datasets, because the more data that can be analyzed, the greater the probability of obtaining accurate results. But to identify correlations and patterns, the qualitative side of these datasets needs to be enhanced in addition to the quantitative side. Big Data analytics tries to achieve this by using algorithms. Big Data includes the entire data management lifecycle of collecting, organizing, and analyzing data to discover patterns, to infer situations or states, to predict and to understand behaviors. The steps of “adding value” to data in a Big Data analytics scenario are usually: Collection from a variety of sources (directly from the data subject or from public or private third Parties), refinement from its raw form, integration with other types of data, preparation for analysis, analytics phase (using data scientists, “Artificial Intelligence” (AI) and machine learning). 32% of all tech companies already use AI and by 2030, with an additional USD 7 trillion in GDP by 2030, China will most likely also be the biggest

⁵² Casalini, F. [Francesca] and López González, J. [Javier]. (2019). *Trade and cross-border data flows*. OECD Publishing. <https://doi.org/10.1787/b2023a47-en>. P. 14–15.

⁵³ Gartner, Inc. (2023). *Gartner Glossary – Big Data*. <https://www.gartner.com/en/information-technology/glossary/big-data>.

⁵⁴ A dataset is a collection of related, discrete items of related data that may be accessed individually or in combination or managed as a whole entity and can be processed as a unit by a computer. It is organized into some type of data structure, e.g., a database. It lists values for each of the variables of the data it includes, e.g.: “EU data holds datasets and services From EU institutions. International data holds datasets and services that comes from beyond the EU. Country data holds datasets and services from the member states of the EU.” Publications Office of the European Union. (2023). *Datasets*. <https://data.europa.eu/data/datasets?locale=en>.

winner of AI implementation in terms of economic gains, followed by North America with only USD 3.7 trillion.⁵⁵

The outputs of these datasets can be used to build predictive models to analyze more data or to make decisions as part of a larger algorithmic or human process. There are therefore many possible applications for these outputs in the areas of development and research, healthcare, risk controlling, marketing, media, smart energy and smart metering, security and traffic, among other fields. Big Data can even support the development of methods for the statistical evaluation of own datasets as part of business intelligence solutions until whole product recommendations for developing or improving a business strategy. The reach of Big Data to valuable datasets has therefore led to an ecosystem in both private and public sectors. Primarily companies in the private sector that have the necessary infrastructure, software, data, and knowledge take advantage of it. This has led to great market power for various companies such as Amazon and has kept the courts busy from an antitrust perspective.⁵⁶ Besides the heavy compliance with data minimization and purpose limitation there is also a lack of transparency due to the complexity of this phenomenon, also because many companies do not openly disclose how they use Big Data in detail. Big Data by its nature may therefore contradict data protection principles⁵⁷ and can pose a considerable risk for the fundamental rights of the data subjects.

In December 1995, an interesting principle was introduced which recognized for the first time the importance of implementing technological capabilities for the purpose of achieving a specific legal effect. This principle, known as “Privacy by Design” determines that in the development and implementation of solutions such as those of Big Data, implications related to data protection must be included in the overall concept. The former Dutch Data Protection Supervisor John Borking developed the underlying idea together with Ann Cavoukian, the former Information and Data Protection Commissioner of the Canadian province of Ottawa, and outlined the main theses of so-called “Privacy Enhancing Technologies” (PETs).⁵⁸ Cavoukian later coined the term Privacy by Design.⁵⁹ In a slightly modified form, Privacy by Design was integrated in Art. 25(1) GDPR. Art. 25(2) GDPR obliges the controller to make “by default privacy-friendly” settings for products, services and applications that limit the collection, processing and transfer of personal data to the minimum required for the specific purpose sought. Privacy by Design and Privacy by Default apply not only at a State or European level but also internationally, as a forward-looking and expedient regulatory concept, to avoid inappropriate further data protection legislation. In December 2015, the “European Union Agency for Network and Information Security” (ENISA) published a study on the design and application of PET in Big Data scenarios.⁶⁰

Another key component of the digital economy is the so-called “Internet of Things” (IoT). IoT can be defined as “encompassing all devices and objects whose state can be read

⁵⁵ Buss, S. [Sebastian]. (2019). *Digital Economy Compass 2019*. Statista GmbH. <https://de.statista.com/statistik/studie/id/52312/dokument/digital-economy-compass/>. P. 45–46.

⁵⁶ Bundeskartellamt. (7 February 2019). *Bundeskartellamt prohibits Facebook from combining user data from different sources*. https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2. // Bodoni, S. [Stephanie]. (30 July 2021). Amazon Gets Record USD 888 Million EU Fine Over Data Violations. *Bloomberg*. <https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach>.

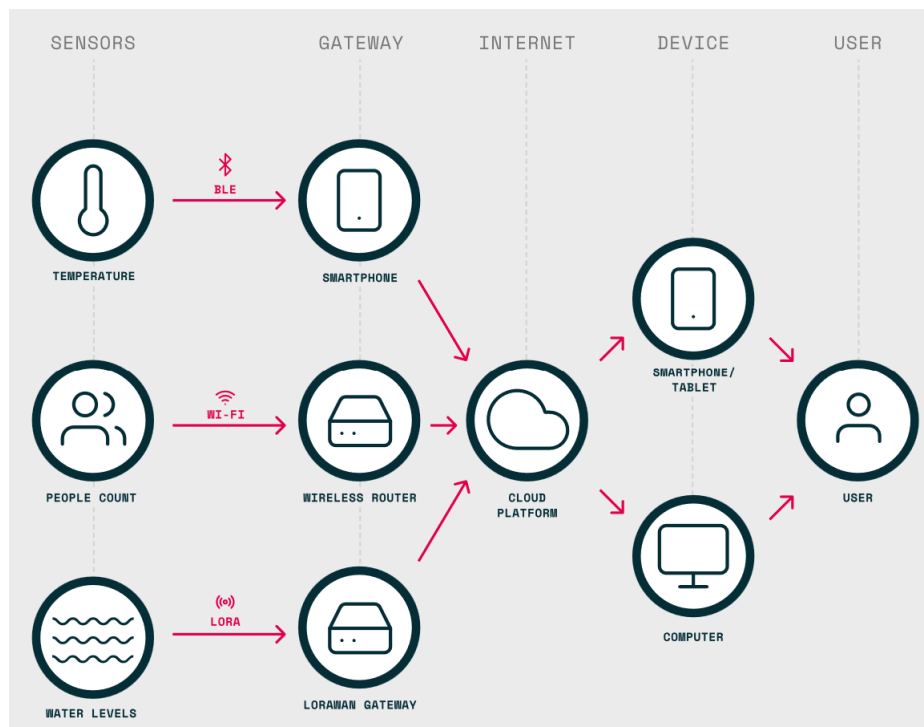
⁵⁷ See also Chapter II, Section II.3.4.3.; and Chapter IX, Section III.2.

⁵⁸ Borking, J. [John]. (1998). *Privacy-enhancing Technologies: The Path to Anonymity*. Registratiekamer.

⁵⁹ Cavoukian, A. [Ann], (January 2011). *Privacy by Design. The 7 Foundational Principles*. <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

⁶⁰ D' Acquisto, G. [Giuseppe] et al. (2015). *Privacy by design in big data*. ENISA. https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport.

or altered via the Internet, with or without the active involvement of individuals”⁶¹. It embeds Internet-connected devices in all sorts of objects and machinery – for example numerical machine tools, buildings, and electro domestics. The rising demand for Internet-connected devices led to an exponential growth in an array of devices with sensors, connectivity, and processing capabilities. The global market for IoT-driven end-user solutions is expected to grow to around USD 1.6 trillion by 2025.⁶² IoT devices monitor a wide variety of processing activities in many economy sectors. Among the most widely used are Smart Cars, Smart Home Appliances and Smart Watches. The dangers of IoT for data subjects are like those of Big Data; however, there are two additional aspects in IoT. First, these devices are more closely linked to the behavior of individuals real life (e.g., at home, at the individual’s body) and thus extend more into their private sphere. Second, IoT relies on different types of embedded sensors, controllers, systems, cloud-based computing services and data communication tools, thus usually links software processes also with hardware, which leads to a complex information service architecture, as the following graphic exemplary shows.



Source: New York City Mayor’s Office of the Chief Technology Officer, “Example of basic IoT system architecture”⁶³

IoT systems can also be used in the context of manufacturing processes. Data has therefore moved into the focus of many companies also in their value chain planning. The so-called “Industry 4.0”⁶⁴ – the fourth industrial revolution after mechanization, division of labor and automation – is a decisive factor for fostering companies’ competitiveness in their markets. It is characterized by the comprehensive, direct networking of “intelligent” objects via the Internet. In addition to the networking of objects, the Commission identifies as further drivers of the transformation process “digital services such as cloud computing” as well as “big data (including data-driven science

⁶¹ OECD. (2015). *OECD Digital Economy Outlook 2015*. OECD Publishing. <https://doi.org/10.1787/9789264232440-en>. P. 61.

⁶² Statista GmbH. (February 2019). *Forecast end-user spending on IoT solutions worldwide from 2017 to 2025*. <https://www.statista.com/statistics/976313/global-iot-market-size>.

⁶³ New York City Mayor’s Office of the Chief Technology Officer. (2021). *IoT Strategy*. https://www1.nyc.gov/assets/cto/downloads/iot-strategy/nyc_iot_strategy.pdf. P. 15.

⁶⁴ Sometimes also called “Manufacturing 4.0”

and geo-spatial data)⁶⁵. Data are also “a medium for the delivery of digitally enabled services across borders, and, with 3D printing, a means of delivering goods; it is an asset that can itself be traded; and an enabler of trade facilitation⁶⁶. The global Industry 4.0 will be relying heavily on IoT, AI, Cloud Computing and Big Data analytics, forming the “big four technologies”; IoT is on the top of the list, with nearly 72% of the respondents to a Statista survey acknowledging that this would be one of the most impactful technologies within their organization.⁶⁷

Those big four technologies led to increased concerns by various stakeholders, including policymakers, consumer associations and data protection experts. These concerns have an international perspective, which developed territorially in particular between the US and the EU. Gasser grouped these concerns into the following three categories: (1) challenges for traditional mechanisms aimed at protecting privacy; (2) new or amplified privacy concerns related to the use of personal data; and (3) cumulative effects of such challenges on trust and technology adoption.⁶⁸ One concern is the anonymization of personal data: The legal obligations under various data protection laws are no longer applicable if personal data is anonymized (respectively “de-identified”). Big Data may involve “so many data points that it may prove too difficult to unlink identities from each piece of data⁶⁹. The second concern is notice and consent: “Many sensors collect information about individuals before they have been notified or asked for consent⁷⁰. Accuracy of data is also affected, because “Big Data algorithms that are used to analyze personal data may not be transparent or understandable to individual subjects [and] IoT devices may have misinterpreted personal information, but recorded and processed it nonetheless⁷¹. Big Data analytics might also lead to an evaluation of a data subject’s future behavior (e.g., propensity for criminal activity) and ultimately to “discriminatory effects and might even violate established antidiscrimination norms and laws⁷². Storage- and purpose limitation are threatened by the fact that “at some point in the future this data could be used for unanticipated purposes⁷³. The obligation to receive consent of the data subjects is therefore “in tension with the trend towards storing more data for unanticipated uses in the future; and [...] the notice and consent model is often criticized for being ineffective in these [Big Data] circumstances”.⁷⁴ This can lead to “users losing the fundamental ability to control the flow of personal information⁷⁵ and endangers the exercise of data subjects’ rights. This could overall result in a lack of trust and consumer confidence and “perceived privacy and security risks may retard the adoption of socially useful Big Data techniques and IoT devices⁷⁶.

⁶⁵ European Commission. (6 May 2015). *A Digital Single Market Strategy for Europe - Analysis and Evidence*. SWD (2015) 100 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0100&from=EN>. P. 58.

⁶⁶ Casalini, F. [Francesca] and López González, J. [Javier]. (2019). *Trade and cross-border data flows*. OECD Publishing. <https://doi.org/10.1787/b2023a47-en>. P. 15.

⁶⁷ Statista GmbH. (2020). *Industry 4.0 technologies expected to have the greatest impact on organizations worldwide as of 2020*. <https://www.statista.com/statistics/1200006/industry-40-technology-greatest-impact-organizations-worldwide>.

⁶⁸ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 350.

⁶⁹ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 351.

⁷⁰ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 352.

⁷¹ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 352.

⁷² Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 353.

⁷³ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 353.

⁷⁴ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 354.

⁷⁵ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 354.

⁷⁶ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 354.

Data are now traded on so-called “data markets” and are essential for businesses. In this regard, Brittany Kaiser, former business development director for “Cambridge Analytica Ltd”, noted that “the wealthiest companies are Tech-Companies. Google, Facebook, Amazon, Tesla. And the reason why these companies are the most powerful companies in the world is that data last years surpassed oil in its value. Data is the most valuable asset on earth. And these companies are valuable because they exploit peoples’ assets.”⁷⁷ The Commission similarly expressed its opinion on the value of the data: “Data has become a new factor of production, an asset and in some transactions a new currency”⁷⁸. Similar comments were also made in China.⁷⁹ The former German Chancellor Ms. Merkel described data as “[...] the raw materials of the 21st century [...]”⁸⁰. There are also considerations⁸¹ to compare data with labor and to assign a property right to personal data in order to protect data subjects from misuse of this – their – asset. Aaronson noted in this respect that “analysts describe data as a form of capital that can be shared and leveraged within and between organizations. They note that data capitalists such as Google, Facebook, Amazon, Uber [...] commodify and monetize data, creating new revenues and/or functions for the company”⁸². Data subjects then “lack bargaining power, and are unable to meaningfully negotiate over payments for our data. Most of us are not sufficiently protected from misuse of our personal data or violations of our privacy. In this way, we are denied a share in the economic value of our data, just as workers in the early industrial age. We are facilitating a massive transfer of wealth from ordinary people to the tech titans.”⁸³ However, Aaronson also correctly stated that treating data like sole capital “exacerbates inequality and limits the productivity gains from big data and AI”.⁸⁴

3. Sociological dimension

In 2016, the number of internet users worldwide was 3.26 billion and for 2022 an amount to 5.28 billion was forecasted.⁸⁵ As of mid-2022, the number of Internet users in Asia was estimated around 2.93 billion against 750 million in Europe.⁸⁶ Data volume of worldwide internet traffic over IP networks raised from 60 Exabyte per month in 2014 to 96 Exabyte per month in 2016 and was expected to reach 396 exabyte per month in 2022.⁸⁷ Data volume of mobile Internet traffic worldwide raised from 2,5 Exabyte per month in 2014 to

⁷⁷ Kaiser, B. [Brittany]. (24 July 2019). *The Great Hack*. Netflix. <https://www.netflix.com/watch/80117542?source=35>.

⁷⁸ European Commission. (6 May 2015). *A Digital Single Market Strategy for Europe - Analysis and Evidence*. SWD (2015) 100 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0100&from=EN>. P. 59.

⁷⁹ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 2.

⁸⁰ dpa Deutsche Presse Agentur GmbH. (12 March 2016). Merkel: Daten sind die Rohstoffe des 21. Jahrhunderts. *Frankfurter Allgemeine Zeitung*. <https://www.faz.net/aktuell/wirtschaft/cebit/angela-merkel-fordert-mehr-modernisierte-digitale-technologien-14120493.html>.

⁸¹ See Chapter VIII, Section II.

⁸² Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 6.

⁸³ Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 6.

⁸⁴ Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 6.

⁸⁵ Statista GmbH. (2023). *Schätzung zur Anzahl der Internetnutzer weltweit für die Jahre 2005 bis 2022*. <https://de.statista.com/statistik/daten/studie/805920/umfrage/anzahl-der-internetnutzer-weltweit>.

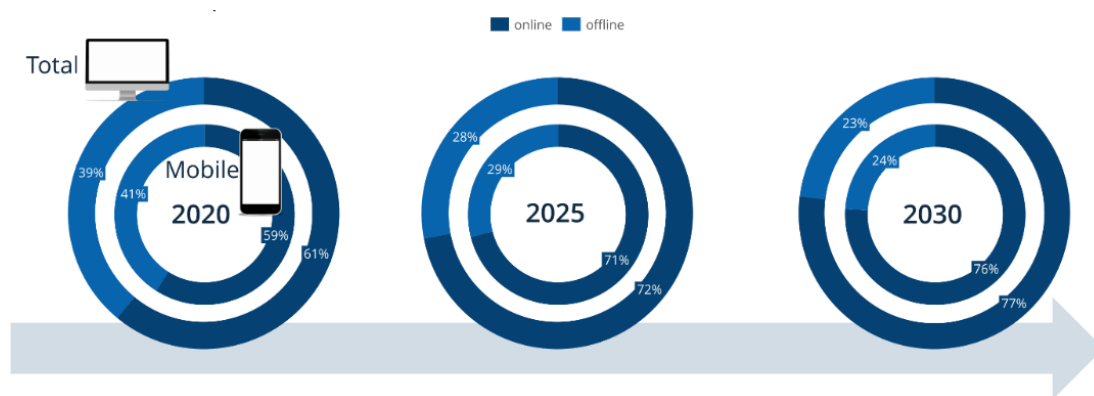
⁸⁶ Statista GmbH. (2023). *Schätzung zur Anzahl der Internetnutzer weltweit nach Regionen im Juni 2022*. <https://de.statista.com/statistik/daten/studie/39490/umfrage/anzahl-der-internetnutzer-weltweit-nach-regionen>.

⁸⁷ Statista GmbH. (2021). *Datenvolumen des globalen IP-Traffics in den Jahren 2014 bis 2017 sowie eine Prognose bis 2022*. <https://de.statista.com/statistik/daten/studie/266869/umfrage/prognose-zum-datenvolumen-des-globalen-ip-traffics>.

7,0 Exabyte in 2016, and was expected to reach 49,0 exabyte per month in 2021.⁸⁸ A 2016 report by the Commission stated that

the Internet now pervades the lives of the vast majority of European citizens: Over 80 % of EU households have broadband connection, up from less than 20 % in 2004; nearly 80 % of EU citizens have smart phones connected to the Internet, up from less than 20 % in 2008; and over 90 % of European businesses are online, with the least connected member state, Romania, quickly catching up to the most advanced, Denmark.⁸⁹

Digitization shapes both professional and private life of a large majority of individuals worldwide and that digitization is going through a process of transformation as more individuals gain access to the Internet.



Source: Statista, "Worldwide Internet penetration"⁹⁰

Such individuals are end users of services of SPs and have specific consumer interests, which range from finding a sufficient variety of services on the market, to transparency of offers, interest in cost-effective conditions, and quality of service. This strengthens the relevance of TFPD. Another reason for an increased social use of TFPD is a so-called "digital convergence". Individuals used to watch films on television or in the cinema, listened to music on a CD player, bought and read printed newspapers, turned on the radio, went in libraries to borrow printed books and talked on landline phones – everything in an "offline" environment. Each sort of media used its own regimes, rules and actors. Nowadays, the Internet is the main choice of medium for those activities, be it on the personal computer, on an electronic reader or on a smartphone. These activities share a common denominator, which is the delivery of content through ISPs. The "World Economic Forum" (WEF) summarized this under the term "Society 5.0", which, through a strong digitization, could transform today's social challenges and found that

societies have evolved from hunter-gatherer (1.0), agrarian (2.0) and industrial (3.0) civilizations to today's information-based (4.0) arrangements. Humankind is now entering into a new "smart" society of sustainable and inclusive socio-economic systems that are powered by big data analytics, AI, IoT and robotics, where digital and physical spaces are tightly integrated. Data could optimize entire societal and welfare

⁸⁸ Statista GmbH. (2021). *Datenvolumen des Internet-Traffics über mobile Endgeräte weltweit in den Jahren 2014 bis 2016 sowie eine Prognose bis 2021*. <https://de.statista.com/statistik/daten/studie/172511/umfrage/prognose-entwicklung-mobiler-datenverkehr/>

⁸⁹ Chase, P. [Peter] et al. (2016). *Transatlantic digital economy and data protection: state-of-play and future implications for the EU's external policies*. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU\(2016\)535006_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf). P. 9.

⁹⁰ Blumtritt, C. [Christoph] et al. (2021). *Digital Economy Compass 2021*. Statista GmbH. <https://de.statista.com/statistik/studie/id/105648/dokument/digital-economy-compass>. P. 21

systems – and not just businesses – that tend to people’s needs at the time and place required, tailored to the individual to improve their quality of life. [But] Digitalization has also caused societal challenges that are linked to new technologies and may expose vulnerable groups to new risks.⁹¹

One of these risks is the so-called “data outing” by individuals through online communities, smart phones and smart device applications. Social media is an integral part of Internet usage not only in the form of social networks, but also forms the link between websites and social media providers. The platforms “YouTube” and “Facebook”, e.g., have a global reach, over 2.5 million users visit each of the two, every month.⁹²

A variety of digital media allow users to interact and create content individually or cooperatively. This interaction involves the mutual exchange of information, opinions, impressions and experiences as well as contributing to the creation of content. Users actively refer to the content through comments, ratings, and recommendations, and build a social relationship with each other. While some individuals care about ubiquitous processing of their personal data, others are insensible to disclose details of their private sphere and tend to assume that they have nothing to hide.⁹³ SPs often do not directly charge a fee for usage; rather, to make their whole business model work, they put their focus on gathering as much personal data as possible to create business income through targeted advertising sales. Meta’s advertising revenue has grown steadily in recent years, reaching around USD 113 million in 2022.⁹⁴ After Facebook achieved 500 million users in 2010, Google was concerned about its own business model, which led to so-called “data wars”, as a platform would possibly get ahead of the other if it would possess more personal data; this also started a period of mayor acquisitions by both Google and Meta (e.g., the companies “DoubleClick” and “WhatsApp”) and triggered advanced tracking measures by both enterprises to make the utmost use of personal data.⁹⁵ As individuals use ISPs more often and are willing to hand over personal data in return for the use of these services, they have become more directly involved in TFPD; not only through E-Commerce but also via participation in social media, which led to a greater level of data exchanges with addressees in other countries. The experience of recent years has shown that non-European platform providers are not properly taking account of European data protection requirements and that EU-based providers depending on these platforms can hardly comply with data protection requirements. This might increase the risk for data subjects participating in such platforms. The processing of personal data of users also plays a prominent role not only in the relationship of enterprises like Meta, Google & Co. to their users, but also in consumer-to-consumer (C2C), business-to-consumer (B2C) and business-to-business (B2B) networks.

To meet the demand of individuals to have their personal data respected, exemplarily, the so-called “right to be forgotten” was enshrined by a judgment of the “Court of Justice of the European Union” (CJEU)⁹⁶ as part of the rights to erasure and to object to the processing of personal data, both laid down in the “Data Protection Directive 95/46/EC”

⁹¹ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 12.

⁹² Statista GmbH. (2023). *Ranking der größten Social Networks und Messenger nach der Anzahl der Nutzer im Januar 2023*. <https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user>.

⁹³ Solove, D. [Daniel]. (2007). I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, Vol. 44, 745-772. P. 747.

⁹⁴ Statista GmbH. (2023). *Werbeumsätze von Meta weltweit in den Jahren 2010 bis 2022*. <https://de.statista.com/statistik/daten/studie/458825/umfrage/werbeeinnahmen-von-facebook/?locale=de>

⁹⁵ Kirk, M. [Michael] et al. (13 May 2014). *United States of Secrets*. WGBH Educational Foundation. <https://www.pbs.org/wgbh/frontline/documentary/united-states-of-secrets>.

⁹⁶ Google Spain case.

(Directive 95/46)⁹⁷. This right is maintained in Art. 17 GDPR, which expressly uses the definition “right to be forgotten”. Under this right, search engine operators are obliged to remove certain results that can be considered personal data through searches made by the name of the data subject. The importance of the ruling lies, on the one hand, in the extension of the territorial scope of European data protection law to non-EU-domiciled companies which operate in the EU and, on the other, in the special emphasis on data protection in relation to public information- and economic interests of data controllers and data processors. It was discussed to what extent website links provided by search engine providers are covered by the right to be forgotten. The “Article 29 Working Party” (WP29)⁹⁸ took the view that a “de-referencing” in search engines should take place worldwide.⁹⁹ Ehmann / Selmayr agreed to this in principle but demanded such an obligation only in the case of a positive proportionality test.¹⁰⁰ With regard to the territorial scope of Art. 17(1) GDPR, the CJEU pleaded for a purely EEA-wide limitation of the deletion obligation according to Art. 17(1) GDPR so that no personal data on servers located outside the EEA/EU would be covered.¹⁰¹ In the opinion of the CJEU, global de-referencing is not required but also not ruled out; the CJEU referred to the possibility for Member States to undertake de-referencing in individual cases insofar as the balancing of interests results in the protection of national norms (especially fundamental rights); it is then up to the search engine operator to take further measures, if necessary, to prevent Internet users in Member States from accessing the extraterritorial links, for example by using so-called “geo-blocking”.¹⁰² This decision affected TFPD to Google’s servers based in the US. Google therefore decided to delete personal data more comprehensively in the future.¹⁰³

The data analysis company Cambridge Analytica had illegally been granted access to personal data of more than 50 million Facebook users during the US 2016 election campaign. These data have helped the company mobilize supporters of Donald Trump while preventing potential Hillary Clinton supporters from voting.¹⁰⁴ About 2.7 million data subjects in Europe were also affected.¹⁰⁵ Facebook was threatened with legal remedies in and outside the US. David Carroll, an associate professor at Parsons School of Design in New York, filed a statement in the high court in London in support of a claim to recover his personal data and reveal their source. In a documentary about the case, Carroll stated that

⁹⁷ EU. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281 (23 November 1995), 31–50. (“Directive 95/46”).

⁹⁸ The “Article 29 Data Protection Working Party” (WP29) is the independent European working group that deals with the protection of personal data. Since 25 May 2018, when the GDPR came into force, it is called the “European Data Protection Board” (EDPB).

⁹⁹ European Commission. (24 January 2020). *WP225 Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12*. <https://ec.europa.eu/newsroom/article29/redirection/document/64437>. P. 3.

¹⁰⁰ Ehmann, E. [Eugen] and Selmayr, M. [Martin]. (2018). *Datenschutz-Grundverordnung: DS-GVO*. C.H. Beck. Art. 17. Para. 37.

¹⁰¹ CJEU. Judgment of the Court (Grand Chamber) of 24 September 2019. *Request for a preliminary ruling under Article 267 TFEU from the Conseil d’État (Council of State, France), made by decision of 19 July 2017, received at the Court on 21 August 2017, in the proceedings Google LLC, successor in law to Google Inc, Case C-507/17*, ECLI:EU:C:2019:772.

¹⁰² CJEU. Judgment of the Court (Grand Chamber) of 24 September 2019. *Request for a preliminary ruling under Article 267 TFEU from the Conseil d’État (Council of State, France), made by decision of 19 July 2017, received at the Court on 21 August 2017, in the proceedings Google LLC, successor in law to Google Inc, Case C-507/17*, ECLI:EU:C:2019:772. Para. 43.

¹⁰³ Google LLC. (6 February 2015). *The Advisory Council to Google on the Right to be Forgotten*. <https://static.googleusercontent.com/media/archive.google.com/en/advisorycouncil/advisement/advisory-report.pdf>.

¹⁰⁴ Rosenberg, M. [Matthew] and Confessore, N. [Nicholas] and Cadwalladr, C. [Carole]. (17 March 2018). *How Trump Consultants Exploited the Facebook Data of Millions*. *The New York Times*. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

¹⁰⁵ de Carbonnel, A. [Alissa]. (6 April 2018). *EU says Facebook confirmed data of 2.7 million Europeans ‘improperly shared’*. *Reuters*. <https://www.reuters.com/article/us-facebook-cambridge-analytica-eu-lette-idUSKCN1HD1AJ>

they [Cambridge Analytica] have not respected the regulator; they are not respecting the law. This is becoming now a criminal matter. We are now in uncharted waters. And I will continue to pursue it because their model has the potential to affect a population, even it is just a tiny slice of a population, because in the United States, only about 70.000 voters in three States decided the election. By the time my daughter is 18, she¹⁰⁶ will have 70.000 data points defining her and currently she has no rights, no control over that at all. So, as individuals, we can limit the flood of data that we are leaking all of the place but there is no silver bullet, there is no way to go off the grid, so you have to understand how your data is affecting your life. Our dignity as humans is at stake.¹⁰⁷

On 30 October 2019, it was announced that Facebook would pay UK authorities a GBP 500,000 fine. UK's supervisory authority, the "Information Commissioner's Office" (ICO), argued that Facebook did not do enough to protect users' personal data and that Facebook had allowed a "serious violation" of applicable law. As the "British Broadcasting Corporation" (BBC) reported, Facebook withdraw the original appeal against the punishment.¹⁰⁸ The company said it wished they had done more to examine Cambridge Analytica earlier. James Dipple-Johnstone, the Deputy Commissioner of the ICO commented: "The ICO's main concern was that UK citizen data was exposed to a serious risk of harm. Protection of personal information and personal privacy is of fundamental importance, not only for the rights of individuals, but also as we now know, for the preservation of a strong democracy".¹⁰⁹ Data Propria, a company run by former officials at Cambridge Analytica, had been working for the "President of the United States of America" (POTUS) Donald Trump's 2020 re-election effort.¹¹⁰ This raised new concerns about a revitalization of a data exploiting model. The WP29 took the Cambridge Analytica scandal as an opportunity to set up a working group especially on social media, which analyzed questions focusing on personal data in social media.¹¹¹ There is therefore discomfort by social media users about scandals related to data protection and trust of data subjects decreased, as also exemplified by three surveys.

Survey on the handling of personal data by Internet services 2018:¹¹² Do Internet services such as Google or Facebook comply with the statutory data protection regulations or do they not comply? Yes: 10%; No: 83%; Don't know: 7%.

Internet privacy concerns 2019 by country worldwide:¹¹³ Share of respondents who are very or slightly concerned about the protection of their data on the Internet in selected countries worldwide in 2018/19.

¹⁰⁶ Throughout the thesis, gender-specific terms may be used to ease the text flow. Whenever a gender-specific term is used, it should be understood as referring to both genders, unless explicitly stated. This is done solely for the purpose of making the text easier to read, and no offense or sexism is intended.

¹⁰⁷ Carroll, D. [David]. (24 July 2019). *The Great Hack*. Netflix. <https://www.netflix.com/watch/80117542?source=35>.

¹⁰⁸ British Broadcasting Corporation. (30 October 2019). Facebook agrees to pay Cambridge Analytica fine to UK. *British Broadcasting Corporation*. <https://www.bbc.com/news/technology-50234141>.

¹⁰⁹ Smout, A. [Alistair]. (30 October 2019). Facebook agrees to pay UK fine over Cambridge Analytica scandal. *Reuters*. <https://www.reuters.com/article/us-facebook-privacy-britain-idCAKBN1X9130>.

¹¹⁰ Horwitz, J. [Jeff]. (15 June 2018). AP: Trump 2020 working with ex-Cambridge Analytica staffers. *Associated Press*. <https://apnews.com/article/north-america-technology-ap-top-news-elections-donald-trump-96928216bdc341ada659447973a688e4>.

¹¹¹ Working Party 29. (11 April 2018). *Sorry is not enough: WP29 establishes a Social Media Working Group*. https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf.

¹¹² Statista GmbH. (24 January 2022). *Halten sich Internet-Dienste wie Google oder Facebook an die gesetzlichen Datenschutzbestimmungen oder halten sie sich nicht daran?*. <https://de.statista.com/statistik/daten/studie/827007/umfrage/umfrage-zum-umgang-mit-persoentlichen-daten-durch-internet-dienste>.

¹¹³ Statista GmbH. (9 December 2021). *Anteil der Befragten, die sehr oder etwas besorgt über den Schutz ihrer Daten im Internet sind, in ausgewählten Ländern weltweit im Jahr 2018/19*. <https://de.statista.com/statistik/daten/studie/1021871/umfrage/bedenken-zum-datenschutz-im-internet-nach-laendern-weltweit>.

Egypt	96%	Brazil	82%	Japan	73%
Hongkong	96%	Russia	82%	Poland	70%
India	92%	Tunisia	80%	France	69%
Nigeria	92%	Turkey	79%	China	68%
Mexico	90%	USA	78%	Germany	68%
South Africa	87%	Canada	76%	Italy	62%
Indonesia	86%	Australia	74%	Sweden	58%
South Korea	86%	UK	73%	Kenia	44%
Pakistan	84%				

Another study showed in 2018 that 76,5 % of German Internet users have concerns about storing personal data with US companies.¹¹⁴

4. Political dimension

The growth of TFPD has also a political significance, especially between the EU and the US. The growing terrorist threat since the terrorist attack on the US on 11 September 2001 (“9/11 attacks”) brought new political challenges to the international community through an increasing demand for surveillance measures. To respond more effectively to the global phenomenon of terrorism, new legislation and anti-terrorism action programs have been developed. Reasoning the “war against terrorism”, far-reaching measures have been taken to combat international terrorism, particularly in the US, but also in other countries, to return to a “strong State” as the answer to this threat. In national legal systems, civil rights have been interfered with in different ways as part of the fight against international terrorism.

An example of US-EU tensions on the stage of politics is the so-called “NSA affair”. Former US “National Security Agency” (NSA) employee Edward Snowden sparked a continuing transatlantic debate over a State’s limitations in the global information society with its revelations about the spying on individuals by the NSA and other intelligence agencies.¹¹⁵ The investigative focus lied on the “PRISM” program, which the US “Privacy and Civil Liberties Oversight Board” (PCLOB) described as follows:

In PRISM collection, the government sends a selector, such as an e-mail address, to a United States-based electronic communications service provider, such as an Internet service provider (“ISP”), and the provider is obliged to give the communications sent to or from that selector to the government. PRISM collection does not include the acquisition of telephone calls. The NSA receives all data collected through PRISM. In addition, the Central Intelligence Agency (“CIA”) and the Federal Bureau of Investigation (“FBI”) each receive a select portion of PRISM collection.¹¹⁶

The NSA collected these data by extracting data from fiber optic cables overseas, where intelligence operations were much less restrained from surveillance laws.¹¹⁷ Google’s internal data lines were not SSL-encrypted by that time. Google changed that after the

¹¹⁴ Web.de. (4 June 2018). *Fünf Jahre nach Snowden: Misstrauen gegenüber US-Anbietern auf Höchstwert Repräsentative Kommunikationsstudie 2018, durchgeführt von Convios Consulting im Auftrag von GMX und WEB.DE.* https://www.slideshare.net/WEBDE_DEUTSCHLAND/fnf-jahre-nach-snowden-misstrauen-im-netz-auf-hchstnivea-100401931/1.

¹¹⁵ Gellman, B. [Barton] and Poitras, L. [Laura]. (7 June 2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

¹¹⁶ ACLU. (2 July 2014). *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.* <https://www.aclu.org/other/pclob-report-surveillance-pursuant-section-702>. P. 7.

¹¹⁷ Kirk, M. [Michael] et al. (13 May 2014). *United States of Secrets.* WGBH Educational Foundation. <https://www.pbs.org/wgbh/frontline/documentary/united-states-of-secrets>.

PRISM functionality had been made public. Google was concerned about the impact on their global competitiveness because its business model is based also on users trust.¹¹⁸ Mr. Snowden had also brought the – similarly functional – “TEMPORA” program of the UK’s “Government Communications Headquarters” (GCHQ) to the attention of a broad public.¹¹⁹ Since 2007, several prominent US-based ISPs had to produce personal data to the NSA.¹²⁰

Wiretapping programs were used even before the 9/11 attacks, with which, for example, telephone data, e-mails or credit card bills were monitored worldwide, including collection from US citizens. However, an automatic anonymization function was integrated in these programs, including the “ThinThread” program, which protected personal data. After the 9/11 attacks, however, this protective function of anonymization was eliminated, so that the subsequent programs prioritized the interests of national security over the right to data protection.¹²¹ The “Trailblazer” program also aimed at comprehensive data mining. However, it did not have protections of personal data in place and, according to NSA whistleblowers such as Thomas Drake, violated the fourth amendment to the US Constitution.^{122, 123}

Another statistic, in this case regarding Germany, underlines the concerns from data subjects raised after the 2013 leaks by Mr. Snowden. This is shown in the result of a survey on data protection concerns in Germany vis-à-vis US-based ISPs from 2010 to 2018. In 2018, 76.5 percent of those surveyed stated that they had data protection concerns vis-à-vis American companies. In 2013, these concerns had increased disproportionately compared to the previous year.¹²⁴

Directive 95/46 raised the European level for the protection of personal data. It provided that the transfer of personal data to a third country may, in principle, take place only if that third country ensures an “adequate level of protection” of personal data. Directive 95/46 also provided that the Commission may find by a so-called “adequacy decisions” that a third country ensures an adequate level of protection. The history of such decisions, which started with Arts. 25 and 26 of Directive 95/46, continued under Art. 45 GDPR. Since Directive 95/46, the regulation of TFPD became increasingly a matter of political significance. Farrell also noted that “privacy – across multiple arenas [...] are inherently political; that is, that they involve conflict between actors with different perceptions of how the good in question is best provided, and even of whether the good should be provided at all”¹²⁵. It was not until relatively late that the US realized what effects the Directive 95/46 would have on TFPD from the EEA to the US. At the same

¹¹⁸ Kirk, M. [Michael] et al. (13 May 2014). *United States of Secrets*. WGBH Educational Foundation. <https://www.pbs.org/wgbh/frontline/documentary/united-states-of-secrets>.

¹¹⁹ MacAskill, E. [Ewan] and Borger, J. [Julian] and Hopkins, N. [Nick]. (21 June 2013). GCHQ taps fibre-optic cables for secret access to world’s communications. *The Guardian*. <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

¹²⁰ Microsoft since 9 November 2007, Yahoo since 3 December 2008, Google since 14 January 2009, Facebook since 6 March 2009, PalTalk since 12 July 2009, Skype since 2 June 2011, AOL since 31 March 2011, Apple since 2012; see Greenwald, G. [Glen]. (2015). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Picador USA. P. 23

¹²¹ Kirk, M. [Michael] et al. (13 May 2014). *United States of Secrets*. WGBH Educational Foundation. <https://www.pbs.org/wgbh/frontline/documentary/united-states-of-secrets>. Stölzel, T. [Thomas]. (10 August 2011). Amerika liest mit. *WirtschaftsWoche*. <https://www.wiwo.de/technologie/spionage-amerika-liest-mit-/5317814.html>.

¹²² USA. *The Constitution of the United States*, (4 March 1789). (“US Constitution”).

¹²³ Shane, S. [Scott]. (9 June 2011). Ex-N.S.A. Aide Gains Plea Deal in Leak Case; Setback to U.S. *The New York Times*. https://www.nytimes.com/2011/06/10/us/10leak.html?_r=2&pagewanted=1&hp.

¹²⁴ Statista GmbH. (10 November 2021). *Anteil der Befragten, die Bedenken haben, ihr privaten Daten bei amerikanischen Unternehmen zu speichern, in Deutschland in den Jahren 2010 bis 2018*. <https://de.statista.com/statistik/daten/studie/869457/umfrage/datenschutzbedenken-gegenueber-amerikanischen-anbietern-von-online-angeboten-in-deutschland>.

¹²⁵ Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US ‘Safe Harbor’ Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield. P. 119.

time, the dilemma arose that the EU's largest trading partner, the US, could not be granted the status of a third country with appropriate data protection safeguards in place. As a result, there was a risk of disrupting all TFPD to the US.¹²⁶

A dialogue was therefore initiated between the US Department of Commerce and the Commission to ensure the adequacy of protection of European citizens' personal data consistent with US preferences for reliance on self-regulation and market mechanisms. This dialogue, which began with the US Department of Commerce proposing a set of data protection principles in November 1998, found a solution on 27 July 2000 when the Commission's adequacy decision was attained according to Art. 25(6) Directive 95/46.¹²⁷ This solution was henceforth called "Safe Harbor Agreement" (Safe Harbor); although it was neither a "bilateral agreement" but validated by that adequacy decision of the Commission, which considered Safe Harbor based on the principles proposed by the US to offer an adequate level of protection; nor was it an "international agreement" but rather two unilateral actions. Safe Harbor was limited to personal data and included principles, which were consistent with OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (OECD Guidelines 1980)¹²⁸ and the Directive 95/46. Safe Harbor required organizations to notify data subjects about the processing of personal data, controls over so-called "onward transfers"¹²⁹, the right for data subjects to "opt out", their right to information and to access their personal data as well as data security and data integrity measures. A US company wishing to join Safe Harbor had to notify the US Department of Commerce and was then placed on a list (the "Safe Harbor List"). From the time of joining, the company had to ensure that the Safe Harbor principles were implemented and practiced in the company. Once joined, the principles were binding for the company until it notified its withdrawal from Safe Harbor to the US Department of Commerce. Enforcement of Safe Harbor was achieved through prosecution by the FTC. When the situation in the US changed with new regulatory instruments after the 9/11 attacks, allowing US public authorities to access stored personal data without the knowledge of the (European) data subject, whose extent Mr. Snowden revealed, criticism on the protection of European citizens' personal data through Safe Harbor raised and the agreement was challenged as potentially void.

A complaint against Facebook brought to the Irish Data Protection Commissioner by an Austrian privacy advocate named Maximilian Schrems was related to those criticisms. In the original complaint from 25 June 2013, Mr. Schrems challenged the transfer of his personal data to the US by Facebook's European-based seat, which is incorporated in Ireland.¹³⁰ The Irish Data Protection Commissioner declined to investigate the complaint, argued to be bound by existing Union law and invoked Safe Harbor. Mr. Schrems appealed this decision before the Irish High Court and the latter referred questions to the CJEU for preliminary ruling ("*Schrems I case*")¹³¹.

¹²⁶ At the end of the 1990s, the transatlantic partners "had entered into a full-blown trade conflict, threatening to disrupt information flows between the largest economic areas in the world. The tensions raised by the directive continue to plague transatlantic information privacy". But not only the US-EU market is affected. The blockage of data flows "hinders the expansion of international trade, especially in the service sectors". See Newman, A. L. [Abraham L.]. (2008). *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Cornell University Press. P. 5.

¹²⁷ European Commission. (25 August 2000). *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*. 2000/520/EC. OJ L 215, 7–47.

¹²⁸ OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/Final, <https://www.uio.no/studier/emner/jus/jus/JUTPRIV/h05/undervisningsmateriale/oecd-pv.doc>, (23 September 1980). ("OECD Guidelines 1980").

¹²⁹ A transfer of personal data to a fourth party or beyond. For instance, the first party is the data subject, the second party is the controller, the third party is the processor, and the fourth party is a sub-contractor of the processor.

¹³⁰ europe-v-facebook.org. (25 June 2013). *Complaint against Facebook Ireland Ltd – 23 "PRISM"*. <http://www.europe-v-facebook.org/prism/facebook.pdf>.

¹³¹ CJEU. Judgment of the Court (Grand Chamber) of 6 October 2015, *Maximilian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650. ("*Schrems I case*").

On 6 October 2015, the CJEU annulled the Commission's decision on Safe Harbor. In essence, the CJEU found that the Commission's findings in its decision as to whether a third country ensures an adequate level of protection, can neither eliminate nor limit the powers of the Member States SAs. Notwithstanding the Commission's decision, these SAs, if dealing with a complaint, would have to assess independently whether the transfer of personal data to a third country meets the requirements of Directive 95/46. The CJEU found also that a regulation allowing US authorities to access the content of electronic communication interferes with the fundamental right to respect for private life; moreover, it found that the fundamental right to effective judicial protection against those activities was interfered because of the lack for EU citizens to appeal that, among other things, their personal data must be corrected or deleted. The CJEU found that the nature of Art. 3 of this adequacy decision is illegitimate in this respect as it reduces the competence of Member States SAs to fully assess the level of data protection of self-certified companies in the US. Although the CJEU ruled that the validity of the adequacy decision of 2000 was not a subject of the referred question itself, it indicated in paras. 93 and 94, that mass surveillance practices of the US are incompatible with European fundamental rights. The CJEU claimed hereby decision-making power on questions of fundamental rights of EU citizens, with which the Commission had formerly dealt with.¹³² After Safe Harbor was annulled, MNEs started to use contractual agreements as an alternative mechanism for TFPD.

Since this ruling did not provide for a transitional period, there fears of a significant impact on TFPD formed a strong political will to create a successor mechanism for lawful TFPD with the US. This will first became known to the public on 15 October 2015 when the vice-president of the Commission and two Commissioners met with business and industry representatives who asked for a clear and uniform interpretation of *Schrems I*. The WP29 published a statement on 16 October 2015 on the consequences of *Schrems I*.¹³³ Therein, it urged Member States to pursue negotiations on an agreement to replace Safe Harbor and suggested an informal grace period of three months during which the SAs would not take enforcement action. After this statement, the Commission issued guidance for companies until a new framework would be put in place.¹³⁴ Therein, it suggested three alternative mechanisms for TFPD with the US: "Standard Data Protection Clauses" (SDPC¹³⁵), "Binding Corporate Rules" (BCR) and the use of derogations set out in the GDPR.

The Commission adopted on 12 July 2016 an adequacy decision¹³⁶, finding that the new mechanism based on the "Privacy Shield" principles¹³⁷ ensures an adequate level of protection. Alike Safe Harbor, Privacy Shield was based on a self-certification system of US companies, with adherence to this mechanism possible since 1 August 2016. Around

¹³² "It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision is valid". CJEU. (6 October 2015). *Press release no. 117/15. The Court of Justice declares that the Commission's US Safe Harbour Decision is*

invalid. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>. P. 2.

¹³³ Working Party 29. (16 October 2015). *Statement of the Article 29 Working Party*. https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

¹³⁴ European Commission. (6 November 2015). *Q&A: Guidance on transatlantic data transfers following the Schrems ruling*. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_6014.

¹³⁵ The abbreviation is used inconsistently in the literature. We follow the text of the GDPR, which in Recital 109, in contrast to the clauses of 2001, 2004, 2010 and 2021, no longer speaks of "Standard Contractual Clauses", but of "Standard Data Protection Clauses". Whenever "SCC" is mentioned in this thesis, then, in the absence of further information, it refers to these SDPC.

¹³⁶ European Commission. (1 August 2016). *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, C/2016/4176, OJ L 207, 1–112.

¹³⁷ U.S. Department of Commerce. (12 April 2023). *EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*. <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>. ("Privacy Shield").

5.300 companies were certified under the Privacy Shield, among them prominent ISPs.¹³⁸

In the period after *Schrems I*, Facebook's EU-based headquarter "Facebook Ireland Ltd" continued TFPD with the US based on SDPC, which were added to a contract between Facebook Ireland and Facebook US.¹³⁹ Mr. Schrems nevertheless conducted further legal actions against Facebook. According to the "Europe vs. Facebook" organization the Irish Data Protection Commissioner followed the objections of the complainant Mr. Schrems in the procedure between Mr. Schrems and Facebook Ireland Ltd. Mr. Schrems claimed that Facebook US continues to be subject to US mass surveillance laws, independent of the use of "model clauses" or "Safe Harbor" and that his data continues to be subject to fundamental rights violations once it reaches the United States.¹⁴⁰

Facebook tried to escape from this criticism with its participation in the Privacy Shield from 30 September 2016 onwards. The resulting new case "*Schrems II*" was the sequel of *Schrems I* and traced back to the end of 2015, when the "Data Protection Officer" (DPO) of Ireland informed Mr. Schrems that Facebook had never actually relied on the now-annulled Safe Harbor agreement but had already relied on SDPC.¹⁴¹ The eleven questions that the Irish Court addressed to the CJEU also included two fundamental questions about the effectiveness of the Privacy Shield. Reacting to this, Advocate General Henrik Saugmandsgaard Øe raised in late 2019 concerns about Privacy Shield, especially its effectiveness of judicial redress.¹⁴² Mr. Schrems welcomed Saugmandsgaard Øe's statement by speaking of a "resounding slap in the face for the Irish Data Protection Agency and for Facebook" and an "important sign for protecting the privacy of users".¹⁴³ In particular, Mr. Schrems continued to believe that "a mere mailbox in the United States Department of State cannot replace a court. Exactly such a court requires the first judgment [*Schrems I*] of the CJEU."¹⁴⁴

The CJEU ruled *Schrems II* on 16 July 2020.¹⁴⁵ The referring court wanted to know whether a "Supervisory Authority" (SA) is bound by the findings in a Commission's adequacy decision. The CJEU found that a SA is generally bound by such decision, but, in the case of a complaint, a SA is nevertheless obliged to an independent examination and, if necessary, to a complaint before the competent national court, so that this court can request the CJEU for a preliminary ruling.¹⁴⁶ The referring court also sought an answer to the question of whether the EU-US Privacy Shield meets the requirements for such an adequacy decision, in particular whether the ombudsman mechanism meets the requirements of Art. 47 of the "Charter of fundamental rights of the European Union" (the Charter)¹⁴⁷.¹⁴⁸ The CJEU ruled that the US legal framework lacks necessary guarantees

¹³⁸ U.S. Department of Commerce. (12 April 2023). *Privacy Shield List*. <https://www.privacyshield.gov/list>.

¹³⁹ europe-v-facebook.org. (27 November 2015). *Letter by Mason Hayes & Curran*. http://www.europe-v-facebook.org/comp_fb_scc.pdf.

¹⁴⁰ europe-v-facebook.org. (25 May 2016). *Rapid Press Update: Facebook & NSA-Surveillance: Following "Safe Harbor" decision, Irish Data Protection Commissioner to bring EU-US data flows before CJEU again*. http://www.europe-v-facebook.org/PA_MCs.pdf.

¹⁴¹ CJEU. *Opinion of Advocate General Saugmandsgaard Oe delivered on 19 December 2019*. C-311/18. ECLI:EU:C:2019:1145. Paras. 45 ff.

¹⁴² CJEU. *Opinion of Advocate General Saugmandsgaard Oe delivered on 19 December 2019*. C-311/18. ECLI:EU:C:2019:1145. Paras. 263 ff.

¹⁴³ NOYB – European Center for Digital Rights. (19 December 2019). *Press release*. https://noyb.eu/sites/default/files/2020-03/pa_ag_19-12-2019_de.pdf.

¹⁴⁴ NOYB – European Center for Digital Rights. (19 December 2019). *Press release*. https://noyb.eu/sites/default/files/2020-03/pa_ag_19-12-2019_de.pdf.

¹⁴⁵ CJEU. Judgment of the Court (Grand Chamber) of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, Case C-311/18, ECLI:EU:C:2020:559. ("*Schrems II* case").

¹⁴⁶ *Schrems II*. Paras. 156 f.

¹⁴⁷ EU. *Charter of fundamental rights of the European Union*, Official Journal of the European Union C 326 (26 October 2012), 391–407. ("Charter")

¹⁴⁸ *Schrems II*. Paras. 161 ff.

for the rights of data subjects as well as effective judicial protection.¹⁴⁹ It held that Section 702 of the “Foreign Intelligence Surveillance Act” (FISA)¹⁵⁰ “cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter” for the reasons that Section 702 “does not indicate any limitations on the power it confers to implement surveillance programs for the purpose of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programs”.¹⁵¹ The CJEU also found that the “Executive Order 12333” (EO 12333)¹⁵², which authorizes access to data in transit to the US without that access being subject to judicial review fails to “delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data”¹⁵³. Furthermore, although the interferences with fundamental rights based on Section 702 are to be carried out in compliance with the Presidential Policy Directive 28 (PPD-28)¹⁵⁴, PPD-28 “does not grant data subjects actionable rights before the courts against the US authorities”¹⁵⁵. The CJEU also examined the role of the US ombudsperson. This organ, directly subordinate to the US Foreign Minister, is part of the executive power, lacks the necessary independence and thus division of powers,¹⁵⁶ and the Ombudsman has no “power to adopt decisions that are binding on intelligence services”.¹⁵⁷ Based on these findings, the CJEU annulled the Privacy Shield decision of the Commission. No transitional period was granted.¹⁵⁸ A TFPD from the EEA to the US based on Privacy Shield was therefore no longer possible. Since SDPC and Privacy Shield were at the time the most frequently used mechanisms for TFPD to the US, many of such flows could not be legitimized – at least temporarily. The general statements made by the CJEU in this respect can also be applied to all third countries without an adequacy decision.¹⁵⁹ Many companies that carried out such transfers to third countries (not only the US), which were not subject to an adequacy decision according to Art. 45 GDPR, were therefore immediately and directly affected by *Schrems II*. A survey underlined this by stating that 48% of the targeted companies in Germany transferred personal data to the US in the past based on Privacy Shield, a 32% naming the need for a political solution for international data transfers as their top priority topic for 2021.¹⁶⁰

Schrems II has taken out the US as a country with “an adequate level of protection within the meaning of paragraph 2 of this Article”, Art. 45(3) GDPR. Therefore, data exporters are generally concerned about which third countries are still “safe countries” under the GDPR and under which conditions. For the assessment of a data exporter before building business cases on TFPD it will therefore become even more important to obtain an understanding of the data protection laws that exist worldwide; this thesis also wants to contribute to this aim. There are considerable doubts as to whether TFPD can still be based on SDPC or other appropriate safeguards within the meaning of Art. 46 GDPR, which ultimately led to the Commission issuing new versions of the SDPC.¹⁶¹ It is also to

¹⁴⁹ *Schrems II*, Para. 168.

¹⁵⁰ USA. *Foreign Intelligence Surveillance Act*, 50 U.S.C. Paras. 1801–11, 1821–29, 1841–46, 1861–62, 1871, (1978). (“FISA”).

¹⁵¹ *Schrems II*, Para. 180.

¹⁵² United States of America. *Executive Order 12333*, US Federal Register, 46 FR 59941, 3 CFR, 1981 Comp., P. 200 (4 December 1981). // See also Chapter III, Section II.1.1.2.

¹⁵³ *Schrems II*, Para. 183.

¹⁵⁴ The White House. *Presidential Policy Directive -- Signals Intelligence Activities*, <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>, (17 January 2014).

¹⁵⁵ *Schrems II*, Para. 181.

¹⁵⁶ *Schrems II*, Para. 195.

¹⁵⁷ *Schrems II*, Para. 196.

¹⁵⁸ *Schrems II*, Para. 202.

¹⁵⁹ EDPB. (23 July 2020). *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*. https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqcjuc31118_en.pdf. P. 4.

¹⁶⁰ Bitkom. (15 September 2021). *Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers*. <https://www.bitkom.org/sites/default/files/2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf>.

¹⁶¹ See below Chapter II, Section II.2.3.4.d.g)

be expected that companies with fewer legal specialist resources in this area will switch to other instruments as legal basis for international transfers of personal data. Because of these burdens for MNEs, the lobbyists' pressure for a solution based on an agreement by political stakeholders is likely to increase. The latest steps at these policy levels were the "Transatlantic agenda" (2020) and the "Trans-Atlantic Data Privacy Framework"¹⁶² (2022) to be analyzed below¹⁶³.

II. Research questions, method, and scope

1. State of the question

When starting this thesis in 2014, developments in the field of international data protection law were both challenge and chance for researchers. Challenge, because many issues affected this topic and constantly broadened its scope; chance because that way, important research on a future regulation of TFPD was still to be done. Research work in this field of law basically arose in three "waves", closely related to the steps in the development of the Internet.

In the first wave, the libertarian idea of a state-free space with unlimited possibilities still prevailed. The Internet should be free of regulation to serve as a space for the global development of individual freedom. Soon after these visions it could be realized that real power structures are hidden behind the dogma of freedom. The public opinion expected behind the US preference for an informal, private-liberal approach to regulation the attempt to secure economic and technical dominance of US companies in cyberspace.

In a second wave, the Internet came into focus as a medium of global development. The elimination of difficulties between "First World", "Second World" and "developing countries" in accessing the Internet was also a focus of the Geneva World Summit on the Information Society of December 2003.¹⁶⁴

Edward Snowden's revelations in 2013 played an important role in the third wave. When he "whistleblowed"¹⁶⁵ to reveal the extensive surveillance programs of the NSA and the UK's GCHQ, a debate started about the role of the Internet in the playing field between participants of digital society and digital economy on the one side, and security and prevention of possible threats on the other.

During the "International Conference of Data Protection and Privacy Commissioners" (ICDPPC) in 2005, a Working Group was set up to deal with global data protection rules. It compared the most important data protection regulations worldwide, tried to identify strengths and weaknesses of the different frameworks and developed a list of data protection rules based on the principles of the various data protection frameworks. The so-called "Global Privacy Standards" emerged, which, however, never attracted significant public attention.¹⁶⁶ This appeal was repeated by DPOs in 2008 at the 30th

¹⁶² The name of this Framework appears to have changed to "EU-US Data Privacy Framework" in 2023, so we will use this name in the following with the abbreviation "EU-US DPF".

¹⁶³ Chapter IX, Section II.1.; and Chapter IX, Section III.3.

¹⁶⁴ International Telecommunication Union. (12 December 2003). *Declaration of Principles, Building the Information Society: a global challenge in the new Millennium*. <https://www.itu.int/net/wsis/docs/geneva/official/dop.html>.

¹⁶⁵ Gellman, B. [Barton] and Poitras, L. [Laura]. (7 June 2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

¹⁶⁶ Cavoukian, A. [Ann], (8 November 2006). *Creation of Global Privacy Standard*. https://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf. P. 1.

ICDPPC in Strasbourg, and at the 31st ICDPPC 2009 in Madrid through the draft¹⁶⁷ of a global legal instrument on data protection with a view to submitting it to the UN. This “Madrid Resolution” made a significant step towards better data protection. The advantage of this resolution was that it was backed by representatives from major MNEs as well as by data protection authorities. This gave it some authority though it remained legally non-binding. The key element of the resolution was that it was based on a higher data protection level of the EU rather than the lowest common denominator, it tended to harmonize up rather than down. Its contents were close to those of EU data protection law, which suggested that it required non-EU data protection levels to be significantly improved. The 32nd ICDPPC of 2010 finally passed a resolution calling for the establishment of an intergovernmental conference to agree on binding international rules on the protection of personal data.¹⁶⁸

Scholarly research took these resolutions as the starting point for their studies. If a global framework for data protection is desirable and, if so, what form it should take, was becoming more relevant because of the growing importance of TFPD in the global digital economy.¹⁶⁹ The constant growth of the capacity of computers, user devices, communication infrastructure and computer analysis and the risks this entails for data protection, as well as a critical view on the future global digital society viewed as a “global village” dominated these discussions. Newman described the radically increased amount of personal data in the global digital economy and put examples of how personal data have become an increasing source of disputes, not only for security issues but also for economic reasons.¹⁷⁰ He argued that European leadership, together with a strong market power, could play a critical role in creating and expanding data protection firstly within Europe and secondly around the world. Poulet underlined the need to analyze data protection as a tool for ensuring both the citizens’ dignity and democracy.¹⁷¹ Among others, Kobrin¹⁷² and Weber¹⁷³ analyzed the challenges and risks of TFPD and provided a historical overview on transnational conflicts regarding personal data, e.g., concerning “Passenger Name Records” (PNR) and data held by the “Society for Worldwide Interbank Financial Telecommunication” (SWIFT)¹⁷⁴.

At the time of starting this thesis, studies had left aside a holistic approach on the international regulation of TFPD, tending to focus on three main issues: (i) the works on the proposal of the GDPR (e.g. Traung¹⁷⁵), (ii) medium-term-oriented policy instruments and practical tools to close the gap between different data protection laws, such as SDPC

¹⁶⁷ ICDPPC. *The Madrid Resolution*, https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf, (2009).

¹⁶⁸ ICDPPC. (29 October 2010). *Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data*. https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolution_international_en.pdf.

¹⁶⁹ Kuner, C. [Christopher]. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25 (4), 307–317. P. 309.

¹⁷⁰ Newman, A. L. [Abraham L.]. (2008). *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Cornell University Press.

¹⁷¹ Poulet, Y. [Yves]. (2009). Data protection legislation: What is at stake for our society and democracy?. *Computer Law & Security Review*, 25(3), 211–226.

¹⁷² Kobrin, S. [Stephen]. (2004). Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 30(1), 111–131.

¹⁷³ Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130.

¹⁷⁴ SWIFT is a cooperative based in Belgium whose members are international banks, stock exchanges and other financial institutions. SWIFT operates its own telecommunications network for a standardized exchange of information among its members, through which several million messages are transferred daily as part of international payments.

¹⁷⁵ Traung, P. [Peter]. (2012). The proposed new EU general data protection regulation. *Computer Law Review International*, 13(2), 33–49.

(Scholz/Lutz¹⁷⁶, Weber/Voigt¹⁷⁷), commissioned data processing agreements (Voigt¹⁷⁸, Funke/Wittmann¹⁷⁹), BCR, Privacy by Design principles (Hustinx¹⁸⁰, Schulz¹⁸¹), and (iii) sector-specific and technology-focused issues of global data protection concerns, such as in cloud computing environments (Blume¹⁸², Ismail¹⁸³, Lanois¹⁸⁴, Schröder/Haag¹⁸⁵), the limits of privacy in automated profiling and data mining (Schermer¹⁸⁶, Weichert¹⁸⁷) and problems of defining applicable data protection law in IT offshoring scenarios (Bäumer/Mara/Meeker¹⁸⁸).

Another aspect that this thesis will analyze is the question of how the EU has been able to promote a comprehensive framework within Europe and how this could help in a global context. To this end we will first follow an historical approach, taking into account, among others, the studies of Newman, who examined the political story and the first legal initiative efforts surrounding the emergence of national privacy laws and the 1990's developments, when EU-wide regulation was pushed forward through different national SAs, ending up with the drafting of Directive 95/46.¹⁸⁹ This achievement led to a rapid global diffusion of European data protection regulations. Kobrin provided an analysis of the historical development of the US legal framework.¹⁹⁰ In addition to the European framework, which has been analyzed by multiple authors¹⁹¹, other supranational frameworks will be considered, such as the "Asia-Pacific" (APAC) Framework.

Regulatory capacity plays an important role in both regional and international politics and has its effects on data protection laws. Newman underlined this idea with a description of the tension between political reactions on societal concerns (e.g., national security issues between US and EU, followed by the discussion around PNR).¹⁹² Bennett/Raab described different policy instruments.¹⁹³ Types of data protection frameworks were also analyzed by Newman. He described comprehensive and limited ones, their institutional features, their implications for society and economy, and considered the variation between the different regimes.

¹⁷⁶ Scholz, M. [Matthias] and Lutz, H. [Holger]. (2011). Standardvertragsklauseln für Auftragsdatenverarbeiter und § 11 BDSG Ein Plädoyer für die Unanwendbarkeit der §§ 11 Abs. 2, 43 Abs. 1 Nr. 2b) BDSG auf die Auftragsverarbeitung außerhalb des EWR. *Computer und Recht*, 27(7), 424–428.

¹⁷⁷ Weber, M. [Marc] and Voigt, P. [Paul]. (2011). Internationale Auftragsdatenverarbeitung - Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln. *Zeitschrift für Datenschutz*, 2011(2), 74–78.

¹⁷⁸ Voigt, P. [Paul]. (2012). Auftragsdatenverarbeitung mit ausländischen Auftragnehmern - Geringere Anforderungen an die Vertragsausgestaltung als im Inland?. *Zeitschrift für Datenschutz*, 2012(12), 546–550.

¹⁷⁹ Funke, M. [Michael] and Wittmann, J. [Jörn]. (2013). Cloud Computing – ein klassischer Fall der Auftragsdatenverarbeitung? Anforderungen an die verantwortliche Stelle. *Zeitschrift für Datenschutz*, 2013(5), 221–228.

¹⁸⁰ Hustinx, P. [Peter]. (2010). Privacy by design: delivering the promises. *Identity in the Information Society*, 3(2), 253–255.

¹⁸¹ Schulz, S. [Sebastian]. (2012). Privacy by Design. *Computer und Recht*, 28(3), 204–208.

¹⁸² Blume, P. [Peter]. (2011). Data Protection in the Cloud. *Computer Law Review International*, 12(3), 76–80.

¹⁸³ Ismail, N. [Noriswadi]. (2011). Cursing the Cloud (or) Controlling the Cloud?. *Computer Law & Security Review*, 27(3), 250–257.

¹⁸⁴ Lanois, P. [Paul]. (2011). Privacy in the age of the cloud. *Journal of Internet law*, 15(6), 3–17.

¹⁸⁵ Schröder, C. [Christian] and Haag, N. [Nils]. (2011). Neue Anforderungen an Cloud Computing für die Praxis. *Zeitschrift für Datenschutz*, 2011(4), 147–152.

¹⁸⁶ Schermer, B. [Bart]. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1), 45–52.

¹⁸⁷ Weichert, T. [Thilo]. (2013). Big Data und Datenschutz. Chancen und Risiken einer neuen Form der Datenanalyse. *Zeitschrift für Datenschutz*, 2013(6), 251–259.

¹⁸⁸ Bäumer, U. [Ulrich] and Mara, P. [Prashant] and Meeker, H. [Heather]. (2012). IT outsourcing and offshoring. *Computer Law Review International*, 13(1), 9–19.

¹⁸⁹ Newman, A. L. [Abraham L.]. (2008). *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Cornell University Press.

¹⁹⁰ Kobrin, S. [Stephen]. (2004). Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 30(1), 111–131.

¹⁹¹ Inter alia: Newman, A. L. [Abraham L.]. (2008). *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Cornell University Press.

¹⁹² Newman, A. L. [Abraham L.]. (2008). *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Cornell University Press.

¹⁹³ Bennett, C. [Colin] and Raab, C. [Charles]. (2006). *The Governance of Privacy*. The MIT Press.

An overview on possible regulatory solutions was provided by Kuner, ranging from international to supranational conventions and treaties, different model laws, non-binding technical standards, international guidelines, recommendations, codes of practice, policy standards, and private-sector instruments.¹⁹⁴ He also drew attention to the key question which international body could lead the development of such regulation.¹⁹⁵

More recently, the legal science focused on problems such as advanced forms of identification (like in the case of smart surveillance systems), Big Data, and jurisdictional issues related to the contradictions between sovereign jurisdiction of States and the ubiquity of the Internet.

Nevertheless, a multitude of problems remain that have so far been insufficiently identified. A more holistic analysis should find a common denominator of these aspects and its effects on TFPD. The absence of this type of analysis underlines the interest of this thesis to put the issue in a bigger context. UNCTAD noted accordingly, that in literature

there is generally a lack of common definitions on data and cross-border data flows. This hampers their measurement, as well as constructive discussion and consensus-building on their governance. Few studies discuss the development implications of cross-border flows of different types and taxonomies of data. Moreover, most of the literature focuses on the trade dimension of data, often neglecting the multidimensional character of data.¹⁹⁶

2. Research questions and hypothesis

The aforementioned relevance of TFPD on the one hand, as well as the absence of a comprehensive study on the regulation of TFPD, raise the question of what the law could offer as an answer to this legal issue. To examine possible answers in this thesis, it is first necessary to determine questions that are to be answered:

- 1) Which are the rules in legal frameworks at global level that affect TFPD? (Chapters I–VII)
- 2) Which problem categories and problem drivers arise from the lack of harmonization in this field of law? (Chapter VIII)
- 3) Within a global ecosystem of TFPD, can regulations be categorized under some framework archetypes, what are the differences between those, and do those have common principles and essential guarantees regarding TFPD? (Chapter IX)
- 4) What objectives and options could a regulatory intervention have? (Chapters X and XI)
- 5) What regulatory content could such intervention have to find a reasonable compromise among the most important stakeholders affected, to act in favor of a worldwide convergence of regulations on TFPD, and how could the process of law-making and enforcement be? (Chapter XII)

¹⁹⁴ Kuner, C. [Christopher]. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25(4), 307–317.

¹⁹⁵ Kuner, C. [Christopher]. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD iLibrary*, No. 187. <https://doi.org/10.1787/5kg0s2fk315f-en>.

¹⁹⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 49.

The hypothesis of this thesis is that a sophisticated combination of legal rules, based on “multi-stakeholder approach” and “blended governance”,¹⁹⁷ will be able to provide for a global consensus on an adequate level of data protection while enabling efficient international flows of personal data. A regulatory intervention should be operationalized by an instrument and an enforcing body:

- The basis for such intervention is the “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (Convention 108)¹⁹⁸ in its modernized version (Convention 108+)¹⁹⁹;
- the bodies to promote and enforce those new rules should be the “United Nations Human Rights Council” (UN HRC) and a new International Court of Justice for Cyberspace Affairs with regional branches.

3. Research objectives

The first objective is to explain what a TFPD is, with all its related scoping terminologies, and why the quantity of such flows has increased, though overall to examine the relevance of such flows viewed from different dimensions.

Other objectives are to analyze current rules at national, regional, and international level which regulate TFPD. In this respect, regulatory instruments of the EU, UN, OECD, “Council of Europe” (CoE), “Asia-Pacific Economic Cooperation” (APEC), and other bodies will be considered. Particularly the contents of three major frameworks, the US and the EU, must be analyzed and outlined to what extent these could form an impetus for harmonized international rules; although China is not considered to be a framework of its one but component of the APAC framework, the domestic legislation in China will also play a role in this analysis due to the emerging importance of China in the global digital economy. Technological solutions will also be of importance as well as regulations developed by the private sector.

The next objective aims at finding out whether the actual status quo is of a sufficiently harmonized nature and if not, what problem categories and underlying problem drivers in the political, societal, economic and technological dimension can be identified.

It is also important to analyze from a comparative law perspective whether there is a common approach within these rules. European regulations set a high level of protection for personal data. In the US and in Asia, the emphasis lies more on self-regulatory approaches. However, the increase in TFPD also influences understandings in these areas and could be of importance to find a “common denominator”. Such a common ground could consist of locating data protection as a fundamental right in international law and acknowledging principles and essential guarantees. Certain typologies of different regulatory approaches will also be discussed and segregated in “archetypes”. The nature of these approaches also depends on different aspects of data protection, its stakeholders and respective interests, as well as “arenas” (or also “games” or “use cases”) in which the aspects of stakeholder management play a role.

The last three Chapters before the final conclusion will be dominated by the analysis whether an international harmonization of TFPD could be reached through an

¹⁹⁷ See in detail below Chapter I, Section II.4.

¹⁹⁸ CoE. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS No. 108 (28 January 1981). (“Convention 108”).

¹⁹⁹ CoE. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223*, CETS No. 223 (10 October 2018). (“Convention 108+”).

international consensus and how such a regulatory solution could be envisioned. Before outlining the possible high-level content of such a regulatory intervention, objectives to solve the remaining problems have to be identified and possible options to be considered.

Harmonization has made some progress at regional level, for example within the EU. It will be outlined how Chapter V of the GDPR is of influence on international transfers of personal data. Such transfers that rely on adequacy decisions or bilateral agreements of the EU with non-EEA countries will also be considered as well as the latest SDPC. Kuner noted that “much important research remains to be done regarding the regulation of transborder data flows”²⁰⁰, and that “there is a nature desire to find a single, high-level solution to the legal issues raised by transborder data flow regulation, and the inability to do so is frustrating”²⁰¹. To analytically accompany the work on an overarching solution is a task to which this doctoral thesis aims to contribute.

4. Methodological approach and workflow

At the center of this thesis lies the best possible solution to harmonize global data protection rules and to remedy the existing shortcomings in the different legal frameworks. Such a harmonization could be achieved by means of a new international legal instrument, which should make global data protection rules as uniform as possible. There are several methodological approaches in pursuing this objective, which relate to the “direction” (“bottom-up” or “top-down”), and to the “intensity” of harmonization. To illustrate these directions, we use on the one hand the international rule of law, a concept of public international law which is legally based and not powerful based. On the other hand, we resort to the risk-based approach under the GDPR.²⁰² In our case, the risk may consist of a *de lege lata* lack of harmonization between the different legal frameworks.

If one were to consider only a harmonizing legislative process at the national level, “bottom-up” would be understood in terms of the involvement of public and private actors influencing this process, such as interest groups and the people as such. In our case, the impetus still ultimately comes from such actors, but this impetus is taken up by a national government and passed on, so to speak, from this nation as a subject of international law to a next higher authority; the latter in our case is the level of public international law. The bottom-up approach for the purpose of this thesis means that the information to identify and assess a risk is to be found in national and supranational²⁰³ laws, which we call “smaller units” of the international hierarchy of norms. Those are also “problem generators” or “problem owners” of a patchwork of data protection laws, as those are not only part of the solution, but also part of the problem. Teubner²⁰⁴, for example, believes that a world law, especially a democratic one, cannot be organized from above, so to speak, by the institutions of international law, but must grow from below. He argues that the (predominantly American-determined) “political-military-moral

²⁰⁰ Kuner, C. [Christopher]. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press. P. 30

²⁰¹ Kuner, C. [Christopher]. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press. P. 186

²⁰² Se Chapter II, Section II.3.4.4.

²⁰³ An important remark must be made for the further course of this thesis: In the literature used, there is often no clear distinction between “supranational” and “regional” laws. We agree with Mireille Hildebrandt who noted that “supranational law differs from international law. In the case of supranational law, a set of Member States have agreed to transfer parts of their sovereignty to a supranational organization”. The most prominent example of supranational law refers to the law of the EU. We generally adhere to the distinction between national law, supranational law and international law. However, because of Chapter IX, which examines certain framework archetypes, it follows that archetypes may refer to certain geographical “regions” or geopolitical “blocks”. Which is why in Chapter XI, Section III., the *termini technici* “regional” and “supra-regional” laws might appear from some sources used. // Hildebrandt, M. [Mireille]. (2020). *Law for Computer Scientists and Other Folk*. Oxford University Press. P. 86.

²⁰⁴ Teubner, G. [Gunther]. (1996). *Globale Bukowina: Zur Emergenz eines transnationalen Rechtspluralismus*. *Rechtshistorisches Journal* 15, 1996, 255–290, P. 255 f.

complex” dedicated to a new world law of peace (“pax americana”) lacks the means of power to control the manifold centrifugal tendencies of a globalized civil society.

We believe that effective risk analysis must also be top-down, because the information from the aforementioned units must ultimately be brought together “centrally” at a subject of international law. Ultimately, aforementioned units would in turn be the addressees of an instrument at international law level. A “central body”, in the words of Rojszczak,²⁰⁵ the “leading role”, then coordinates, assists, and ensures, among other things, a uniform procedure for risk analysis and a common understanding of the procedure and assessments.

We therefore agree with Röhl, who countered Teubner’s view:

It is certainly correct to observe processes of the globalization of legal development and thus also of the globalization of law at their social basis, if only because official law is much more obvious anyway. On the other hand, it seems out of the question to weigh the system performance of law and politics in comparison to the performance of the social peripheries. The two cannot be compared at all but can only be described in terms of their interaction or opposition. It is therefore better to refrain from an overall assessment and to describe in detail the contributions made to the globalization process by social actors and those actors acting in the political or legal system. After all, such descriptions show that some areas that initially practice a more or less successful self-regulation end up being integrated by official law. This is true, for example, for the Internet or for corporate social responsibility.²⁰⁶

Moreover, because this “direction” is fluent and can change. Hildebrandt also correctly noted that

International law depends on national law. First, because national law determines to what extent states are bound by international law. Second, because enforcement of international law depends on national bodies (legislature, courts, administration). This implies that international law, to a large extent, depends on states willing to bind themselves. There are some exceptions, for example, with regard to *ius cogens*, which applies whether or not states recognize its force. [...] However, national law also depends on international law. First, because the system of sovereign states is based on mutual recognition of each other’s internal and external sovereignty. [...] Without external sovereignty, which depends on the international legal order, we cannot “have” internal sovereignty²⁰⁷

We therefore think that the picture of national / supranational laws must be supplemented by a public international law perspective, especially when it comes to a necessary transfer of sovereignty from the national / supranational level to the international level, which is what is needed, at least in part, for harmonization at the international level. This makes our approach overall top-down, with a recognition of bottom-up elements.

Second, the “intensity” of harmonization must be determined. During the work on this thesis, we have found that a wide variety of sources do not make a clear distinction between “harmonization”, “approximation”, standardization”, “unification”, and similar *termini technici*. Speaking of methodology, we see at least a necessary distinction

²⁰⁵ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 36. // See also below Chapter XI, Section III.

²⁰⁶ Röhl, K. [Klaus]. (2006). *Rechtssoziologie: Ein Lehrbuch*. Carl Heymanns. § 96. III. 1.

²⁰⁷ Hildebrandt, M. [Mireille]. (2020). *Law for Computer Scientists and Other Folk*. Oxford University Press. P. 93–94

between “harmonization” on the one hand and “unification” on the other. Their difference lies in the degree of “strictness”, respectively their binding effect, whilst striving for the optimum of uniformity. Harmonization involves a reduction in “variations”²⁰⁸, while unification requires moving towards the eradication of any variation. In the present thesis, the ambition is the determination of a “level” of data protection rules as uniform as possible; this means as aligned as possible, with the fewest possible variations, in the ideal case by means of a single regulatory text. This comes with an adjustment of differences and inconsistencies among different legal systems to make them at least more compatible. To determine which rulesets should be adjusted towards each other, it is necessary to identify the “sources” of such diversity so that the potential of comparability of the global framework can be evaluated.

These sources can also be “standards”. ISO/IEC 27001:2022, e.g., expresses that standards serve the purpose of unification and harmonization and are desired or essential characteristics that are elevated to the status of a standard, e.g., measurement methods (temperature), products (dimensions), and communication protocols (HTTP). Harmonization does not exclude the use of standards but tries to find the best compromise between too many and too few standards for a certain process. This process seeks to minimize redundant or conflicting sources. Standards do not necessarily represent a concrete regulation and can have the function of a guideline and be a model for a legal standard of behavior. Building on these considerations, “data protection standards” are understood in this thesis as a largely uniform – legislative or non-legislative – approach to data protection issues, based on which users of such standards are guided. Regarding these standards, the term “standardization” will also be of importance in this thesis. Nevertheless, we do not expect a full “unification” of global data protection law by completely eradicating all differences. The level of data protection to be proposed leaves differences in national laws in place where those are not expressly addressed by the legal instrument to be proposed, like the so-called “opening clauses” of the GDPR. We expect that some variations need to be allowed, but not all, because the latter would be the other (too) “extreme”²⁰⁹. We will seek the highest possible level of harmonization of the laws to be analyzed in the FIRST PART of this thesis through the aforementioned new instrument but those laws not to be fully “unified” in the sense of being “identical”.

4.1. International and comparative law

In addition to the mentioned approaches on direction and intensity, a relevant aspect of the methodology of this thesis relates to dealing with different jurisdictions and legal frameworks. International law is indispensable for the comparative part of this thesis, as it relies on legal sources such as Art. 38 of the Statutes of the “International Court of Justice” (ICJ).²¹⁰ Comparative law contributes to a spatially and factually limited approximation of legal systems to minimize the risks associated with the application of foreign law. It is important to determine the necessary level of protection which is agreed upon and which then could possibly lead to a harmonization of the relevant legal rules, a determination that relies on the discipline of comparative law. To justify the harmonization goal set out in this thesis, it might be sufficient to show differences

²⁰⁸ This could also be called “deviation”. Nevertheless, we think “variation” is a better fit at this point, because this term encompasses more the “output” or “result” of, e.g., within EU law, the aim of harmonization but allowing deviations of national law from supranational law. // Hunt, J. [Jo]. (2010). Devolution and differentiation: Regional variation in EU law. *Legal Studies*, 30(3), 421–441. P. 422.

²⁰⁹ In a sense that a regulatory intervention at the international law level could not be achieved due to lack of consensus, because “extreme positions” of Parties to be included in that intervention might endanger to meet the objectives of that intervention.

²¹⁰ ICJ. *Statute of the International Court of Justice*, (1945).

between the legal systems without requiring an in-depth assessment of the content of these regulatory differences in terms of a comparison of minimum levels. Another facet of approximation of laws could be, if appropriate, to approximate rules towards others applicable in the States concerned. This corresponds to the classic use of a comparative approach to international lawmaking.²¹¹

EU secondary law, with Directives and Regulations, could serve as a blueprint for such harmonization. The relevance of a comparative law method becomes apparent when looking at the juxtaposition of national private law systems in Europe, especially in EU Member States, which have provided extensive material for comparative law during the development period of the EU, which have also stimulated each other. However, globalization has raised new norm producers and diverse processes of norm creation. States organize themselves in “blocks” (e.g., EU, APAC). Those States set autonomous law and strive for harmonization in their market. This results in national law becoming less relevant. The dialogue between supranational and national law is not unchallenging, as different traditions and conceptions of regulation clash. Comparative law could dissolve this challenge, as it could assess the compatibility of supranational law in the national environment and remove obstacles. It could ensure that national law remains functional even under the pressure to align with supranational rules. In addition, it could prevent globalization from degenerating from a dialogue between different legal cultures into the hegemony of a single legal culture (e.g., a so-called “Europeanization of data protection law”²¹²).

A practical example of how to deal with legal harmonization could be found in the actions taken by the Commission when the “European Parliament” (the Parliament) called to submit a study on harmonization in the field of civil law in 2000.²¹³ In its 2001 Communication on Contract Law, the Commission asked consumers, practitioners, academics and State institutions for comments on the need to approximate contractual rights in Europe, related problems and possible solutions.²¹⁴ In its action plan for a more consistent European contract law in 2003, the Commission expanded its initial approach of a mere juxtaposition of legal systems.²¹⁵ The area of comparison was enlarged beyond the traditional comparative law by including uniform private law, in the form of existing regulations of the “European Community” (EC) at the time, as well as international instruments such as the “United Nations Convention on Contracts for the International Sale of Goods” (CISG).²¹⁶ Since international instruments are based on a consensus and are of a more neutral nature, the Commission expected that the regulations contained therein could be more likely to be accepted by the concerned Member States.

²¹¹ Kropholler, J. [Jan]. (1975). *Internationales Einheitsrecht*. Mohr Siebeck. P. 254 ff.

²¹² Lynskey, O. [Orla]. (2017). The ‘Europeanisation’ of Data Protection Law. *Cambridge Yearbook of European Legal Studies*, 19, 252–286.

²¹³ European Parliament. *European Parliament resolution on the Commission’s annual legislative program for 2000*, Official Journal of the European Communities, C 377/323, (2000). Para. 28.

²¹⁴ Option I: No action by the European Communities. This would follow the market economy idea that self-regulation is better than sovereign intervention. Option II: Approximation of national legal systems through common principles. This could lead to the application of non-governmental legal texts. Option III: Improve existing legislation. This is not a deviation from the previous procedure and should actually be a self-evident goal of every legislator. Option IV: Elaboration and enactment of new regulations. These could take the shape of regulations that are binding for the signatory States according to Art. 249 III of the Treaty of Rome, or EEC Treaty (officially the Treaty establishing the European Economic Community), regulations binding for the citizens according to Art. 249 II EEC Treaty or non-binding recommendations and statements according to Art. 249 V EEC Treaty. // Commission of the European Communities. *Communication from the Commission to the Council and the European Parliament on European contract law*, COM/2001/0398 final, 15–18, (2001).

²¹⁵ Commission of the European Communities. *Communication from the Commission to the European Parliament and the Council - A more coherent European contract law - An action plan*, Official Journal of the European Union C 63/1, (2003).

²¹⁶ Commission of the European Communities. *Communication from the Commission to the European Parliament and the Council - A more coherent European contract law - An action plan*, Official Journal of the European Union C 63/1, (2003). Para. 63.

4.2. Cross-disciplinary and functional approach

TFPD not only lead to various intersections within the global information society in the real world, but also interact with many different elements of the legal sphere. Therefore, it is important to describe which connection comparative law has to other legal disciplines and approaches. Sometimes a differentiation is possible, sometimes this relationship can be so close that all disciplines affected cannot be suitably applied without one another.

Philosophy of law and comparative law have in common the search for principles that stand behind the rules of human behavior, the sensing of hidden solutions. With the search for meaning, origin and essence of law, the philosopher's range of questions goes beyond that of the legal comparator. The main difference, however, lies in the methodical approach. Comparative law works empirically and inductively, in that it tries to distill the solution from legal systems based on legal reality. The philosophy of law starts with the legal ideal ("should-do") and looks for ways to reach that ideal within the legal reality. The boundaries of comparative law are becoming increasingly blurred regarding the fields of legal history, legal sociology and legal ethnology. Legal history cannot do without the comparison with current law, and comparative law must consider the historical conditions under which the legal norms in comparison have developed. Legal ethnology can then be viewed as a branch of comparative law if it deals with the external pressure on the legal relations of traditional societies (e.g., the raise of new cultures). Legal sociology is the study of the relationships between society and law; it wants to determine the controllability of human behavior through norms and to study the norms' reactions to social change. For the elaboration of what are to be considered "essential values" in the area of data protection, all aforementioned disciplines of the law are to be considered in this thesis.

There is a need to address the purpose of this thesis as a complex issue, whereas any solution shall be built on the grounds of a cross-disciplinary research. The core argument for this is – with Gasser – that

the current digital privacy crisis and resulting challenges need to be seen in context and as part of deeper-layered tectonic shifts in the ways in which information is created, shared, accessed, and used in the globalized digital world. These shifts, in turn, are the result of a complex interplay among technical, economic, behavioral and normative forces. Interdisciplinary knowledge is not only needed to better understand and analyze the origins and dimensions of today's privacy crisis, but is also required when mapping the solution space and considering the future of digital privacy, especially from a legal and policy perspective and in the sense of a mixed governance approach.²¹⁷

If the approach of this thesis is at all close to a special comparative law method, so is this the "functional method". Because – with Kischel²¹⁸ – we consider the commitment to one solely comparative law method for the subject of this thesis to be unrealistic. We will therefore provide a mixture of non-legislative and legislative measures to solve problems²¹⁹ that have yet to be identified within the four dimensions of relevance mentioned above²²⁰.

²¹⁷ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 340–341.

²¹⁸ Kischel, U. [Uwe]. (2019). *Comparative law*. Oxford University Press. Chapter I, Paras. 14–16.

²¹⁹ See Chapter VIII

²²⁰ Chapter I, Section I.

In this thesis, a fundamental rights law perspective will be given preference over a trade law perspective.²²¹ An UNCTAD assessment underlines our opinion by stating that

a sizable share of research focuses on data and trade, especially with respect to shaping international rules within trade negotiations. This is certainly an important topic for cross-border data flows. However, both Burri (2016) and Mattoo and Meltzer (2018) reject the idea that these flows should be negotiated within the realm of trade negotiations, as they are either too one-sided or leave out relevant actors, such as the Internet governance community.²²²

Granted, even though the “Charter of the United Nations” (UN Charter)²²³ is universal, it can be interpreted differently in certain countries. However, the fundamental rights perspective would have its advantages even then, because “the assessment of the fundamental rights position becomes useful as it mandates courts to take all positions and interests into account and thus avoids one-sided approaches”.²²⁴

In our view, a functional method should correspond to interdisciplinary forces explained by Gasser. He calls what he sees as the necessary approach to regulating such forces a “blended governance”. He wants to take a “broader governance approach rather than a strictly law-based approach”²²⁵ by examining four different modes of response.

First, technological approaches such as Privacy Enhancing Technologies and Privacy by Design are considered. Second, [...] the possible role of market forces and other market-based mechanisms – such as the reputation of a company – when addressing the privacy challenges of our time. Third, a series of human-centered responses to the privacy crisis are discussed, ranging from user education and empowerment to concepts derived from behavioral economics, such as nudging. Finally, traditional and non-traditional legal approaches are examined as a way to not only address the digital privacy crisis, but also potentially coordinate or shape the other governance mechanisms discussed in this section. [...] There is no silver bullet solution and instead explores the contours of a framework for blended governance, necessitated by a highly interconnected, complex, and uncertain world in which the role of information - including personal data - and the importance of information flows will only increase over time.²²⁶

The principle of functionality within comparative law means that those legal norms that are functionally related should be compared because they address the same factual problem. The aim should therefore be to find functional equivalents in legal systems. Since, however, the consideration of all legal systems worldwide is not possible under the specifications of the scope of this thesis, the States which best reflect the relevant legal approaches around TFPD are to be considered. Since the hypothesis of the work includes the need for harmonization, a comparative part may not end at this point but also evaluate the effectiveness of an approach to the legal problem in the context of the sociological, technological, economic and political peculiarities of a legal system.

²²¹ See also Chapter X, Section II.3.

²²² UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 60–61.

²²³ The UN Charter encompasses the UDHR, the ICCPR and the Statutes of its organs, such as the ICJ. // UN. *Charter of the United Nations and Statute of the International Court of Justice*, (1945).

²²⁴ Wielsch, Dan. (2008). *Zugangsregeln: die Rechtsverfassung der Wissensteilung*. Mohr Siebeck. P. 66-81.

²²⁵ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 341.

²²⁶ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 341–342.

Three other proponents of this functional approach are therefore considered. First, as Sacco²²⁷ noted, case law must be considered in addition to legislation, because legal norms of two (exemplary) States may be similar or the same, but courts of different States may decide differently based on the legal norms. Secondly, with Kamba²²⁸, an approach focusing on the examination of the formal norms, institutions and concepts in one legal system might be misleading for the connection between law and society, since such focus “may not disclose corresponding categories in another system”; it is important to look for “what legal norms, concepts or institutions in one system perform the equivalent functions performed by certain legal norms, concepts or institutions of another system”. Thirdly, with Constantinesco²²⁹, a comparative process is divided into three phases, “ascertaining, understanding, and comparing”. These three steps will shape the structure of this thesis. The first step is to establish how the compared legal systems treat the legal issue, to which the FIRST PART will be devoted. In the second step, the issue to be compared is to be incorporated into the legal system in question. To do this, however, the overarching problems must first be determined (Chapter VIII) and which framework archetypes come into question (Chapter IX). Only then the legal systems under consideration can be compared with each other by determining differences and similarities, to ultimately establish what relationship the compared legal issues have to each other.

Chapter I starts the investigative process in this interdisciplinary environment to finally be able to determine, in Chapter XII, which solution may be proposed. This process is essentially divided into “the run-up to a proposition” and “the proposition itself”. For the former (up to and including Chapter XI), a “general methodology” of decision-making in everyday life, and, on the other hand, a “specific methodology” in the field of law-making, will be used.

4.3. General proposition-making and specific proposition-making methodologies

The “general” methodology is based on seven “W-questions”, which are known from journalism’s news style and go back to Aristotle’s *Nicomachean Ethics*: What, When, Where, Why, What for, How, Who.²³⁰ This questioning technique ensures that “users” of the technique – i.e., both the author and the readers of this thesis – have a complete picture of the situation, by guaranteeing that all information is available. In the case of this thesis, it is ultimately about information to be transported until Chapter XII. “What?, When?, and Where?” are determined in Chapter I by the research questions, research objectives, as well as by the scoping terminologies. “Why?” commences in Chapter I with the “dimensions” and is continued by the elaboration of the current data protection regulations (FIRST PART), a classification of problems in Chapter VIII, and the presentation of commonalities and differences in legal systems (Chapter IX). “Who?” turns to the stakeholders in the ecosystem of TFPD. “What for?” builds on the hypothesis of thesis; the goals are sharpened by the “objectives” in Chapter X. “How?” is delineated by the various theoretical “options” in Chapter XI.

²²⁷ Sacco, R. [Rodolfo]. (1991). Legal Formants: A Dynamic Approach to Comparative Law. *The American Journal of Comparative Law*, 39(1), 1–34. P. 23.

²²⁸ Kamba, W. [Walter]. (1974). Comparative Law: A Theoretical Framework. *International and Comparative Law Quarterly*, 23(3), 485–519. P. 517.

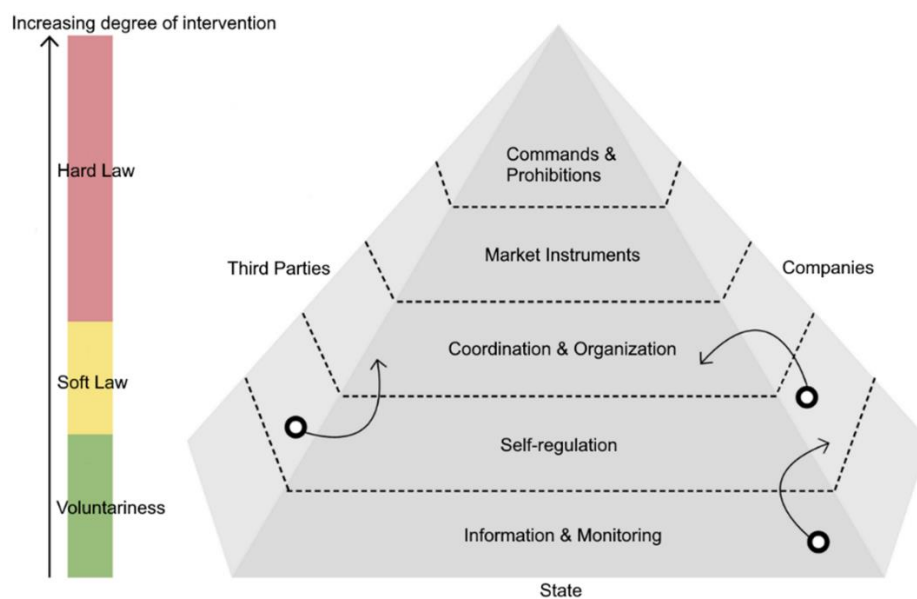
²²⁹ Constantinesco, L.-J. [Léontin-Jean]. (1972). *Die rechtsvergleichende Methode*. Vol. 2. Heymanns. P. 137–139.

²³⁰ Sloan, M. [Michael]. (2010). Aristotle’s *Nicomachean Ethics* as the Original Locus for the *Septem Circumstantiae*. *Classical Philology*, 105(3), 236–251. P. 236.

This general methodology is supported by the “specific” methodology. The latter concerns the question of whether a legal issue should be regulated at all. Only when the answer is “yes” and the objectives of a regulatory intervention have been determined, the question of “how” arises. It must be clarified how a regulatory intervention could be best designed. This requires answering questions about what constitutes “better legislation”, if not “good legislation” at all; and about the “effectiveness” of such regulation (e.g., causing the lowest possible costs and harmful side effects). Also questions about clarity and comprehensibility of norms; or even about abandoning regulation all together? The latter is what some might like to demand, given the complexity of the subject-matter, but one might then be confronted with the question of how this abandonment would relate to the so-called “theory of materiality”, which says that the rule of law and the principle of democracy require the legislature to make all essential decisions for a regulatory area itself and not to leave them to the executive branch within the separation of powers.

4.4. Smart Regulation and Better Regulation approaches

There are several approaches to a “Regulatory Impact Assessment” (RIA) as a prerequisite for the best possible fulfillment of quality requirements for legislation. There is a concept from 1998 to be considered, the so-called “Smart Regulation”²³¹. This concept includes smart regulation principles²³², which compose a “regulation pyramid”.



Source: Leimbacher, J. [Jörg], “Smart Regulation, Regulation Pyramid”²³³

²³¹ Gunningham, N. [Neil] and Grabosky, P. [Peter]. (1998). *Smart Regulation: Designing Environmental Policy*. Clarendon Press.

²³² 1) Instruments with little government influence are to be preferred, 2) The regulatory system is ideally designed as a cascade or sequence of stages, 3) An optimal mix of instruments can increase effectiveness, 4) Affected non-state actors should be involved, 5) Flexible instruments can offer opportunities for the economy and at the same time effectiveness.

²³³ Adapted from: Leimbacher, J. [Jörg]. *Smart Regulation: Kurzfassung*. (2021). <https://www.aramis.admin.ch/Default?DocumentID=68333&Load=true>. P. 7.

In addition to Smart Regulation, the concept of “Better Regulation” is also a central point of reference for the regulatory policy in the OECD²³⁴, the EU²³⁵, and beyond, and will be considered in this thesis. In particular, the “Europeanization of national legislation” has brought with it new questions in this respect. The Commission has recognized the need to promote openness and transparency in the EU decision-making process, to improve the quality of new legislation through better RIAs of draft legislation and proposed amendments, and to ensure a continuous and coherent review of existing EU law to achieve the objectives of EU action as effectively and efficiently as possible. Therefore, the Commission introduced changes to its Better Regulation policy to “set out the principles that the European Commission follows when preparing new initiatives and proposals and when managing and evaluating existing legislation”²³⁶. This policy is based on three documents. Firstly, communications from the Commission, secondly, the guidelines, and finally, a so-called “toolbox”. In November 2021, the Commission adopted new guidelines²³⁷ for better regulation and a new toolbox²³⁸. These guidelines were based on the key aspects outlined in a Commission’s communication²³⁹ of 29 April 2021, which announced a new generation of Better Regulation. Particularly within elements of the “Digital Strategy”²⁴⁰, the Commission elaborated considerable RIAs such as the one for the proposed “E-Evidence Regulation”²⁴¹.

While Smart Regulation focuses on the design of a regulatory text as such, Better Regulation encompasses principles for optimizing the entire policy-making process in all phases of the creation and implementation of a regulation. The Better Regulation approach starts with an “Inception Impact Assessment”, including an initial assessment of possible impacts and options, consulted for 4 weeks; problems and problem drivers are outlined in this phase. Following this phase, the Commission conducts a public consultation of 12 weeks during the elaboration of a RIA. Concerns of citizens are then usually obtained once the potential legislator had previously outlined problems. Legislative proposals and the accompanying final RIA are then published for feedback for another 8 weeks following the approval of the proposal. Stakeholder interests are considered by the Commission throughout the whole elaboration of a RIA.

In the systematic examination of the possible effects of a regulation, this thesis will also incorporate a consideration of stakeholder interests. As can be seen from the following graphic, Better Regulation puts those interests in the center.

²³⁴ OECD. (2012). *Recommendation of the Council on Regulatory Policy and Governance*. <https://www.oecd.org/governance/regulatory-policy/2012-recommendation.htm>. // OECD. (2020). *Regulatory Impact Assessment*. <https://www.oecd.org/gov/regulatory-policy/regulatory-impact-assessment-7a9638cb-en.htm>. // *Nota bene*: The Principles within the RIA complement the 2012 Recommendation.

²³⁵ European Commission. *Better regulation toolbox - November 2021 edition*. https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). // *Nota bene*: This toolbox complements the better regulation guidelines presented in SWD(2021) 305 final.

²³⁶ European Commission. *Better regulation: guidelines and toolbox*. https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en, (2021).

²³⁷ European Commission. *Better Regulation Guidelines*, SWD(2021) 305 final, (2021). // *Nota bene*: This version replaced the 2017 version SWD(2017) 350.

²³⁸ European Commission. *Better regulation toolbox - November 2021 edition*. https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021).

²³⁹ European Commission. *Better Regulation – joining forces to make better laws*, COM(2021)219, (2021).

²⁴⁰ See in detail below Chapter II, Section II.3.8.2.

²⁴¹ European Commission. *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*, Official Journal of the European Union, L 295/39, (23 October 2018).



Source: European Commission, “EU policy and law-making cycle”²⁴²

The examination and balancing of these underlying stakeholder interests is one of the main subjects of this thesis. Moreover, “the Commission’s better regulation system is one of the most advanced regulatory approaches in the world”²⁴³ and “the OECD considers that the Commission has the best approach to consultation”²⁴⁴. The Better Regulation approach is therefore preferred as the specific methodology for this thesis.

5. Scoping terminologies

This work will be limited to transborder flows through which personal data are transferred. Terminology is inconsistent in the field of international data protection law and makes a closer examination necessary. The UN noted similarly that

the scope of the topic *ratione materiae* would be a matter that would require careful consideration, in particular whether it should be only automated computerized data, or any kind of data, including manually generated and data; and whether the scope should be defined through the technology used or through any kind of data involved regardless of the technology. It would be necessary to define such terms as data; data-subject; data user; data file; data retention; data preservation; personally identifiable data; sensitive data; traffic data; location data; transborder flow of personal data; processing of personal data; communication; third party user; registration and transactional data; clickstream data. The definitions are only illustrative; they need to take into account the technological advances that are continuously taking place in the network environment.²⁴⁵

According to those rapid technological advances, a variety exists as to what is understood by different terms in this area, as also UNCTAD resumed: “Defining data better – and the areas of economies, societies and the overall environment they touch upon – is important to further the discussions on measurement, as well as on their policy implications”.²⁴⁶

²⁴² European Commission. (2022). *Bessere Rechtsetzung – warum und wie?*. https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation_de.

²⁴³ European Commission. *Better Regulation – joining forces to make better laws*, COM(2021)219, (2021). P. 1.

²⁴⁴ European Commission. *Better Regulation – joining forces to make better laws*, COM(2021)219, (2021). P. 4.

²⁴⁵ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Paras. 21-22

²⁴⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 60.

5.1. Personal Data

Regulatory instruments which have only the processing of non-personal data in scope, fall out of the scope of this thesis. However, there are difficulties in determining in a scientifically meaningful way which transborder flows at the global level contain personal data or non-personal data, and in which parts. This is supported by Aaronson, who noted that “a large amount of the data exchanged across borders is personal data. However, there are no reliable statistics about the types of data exchanged across borders and what percentage is personal.”²⁴⁷ Steinrötter noted that “the economic reality is that datasets and data flows often contain both personal and non-personal data”.²⁴⁸ Moreover, and probably because of this scientific difficulty, some sources of this thesis are not explicitly related to personal data only but focus on non-personal data as well as personal data. Others only hint at such inclusion. For the remainder of this thesis, it is therefore important to note that whenever “data” are referred to without explicitly distinguishing between non-personal and personal, personal data are to be understood as inclusive.

The Commission stated in its Data Strategy that, in order to deal with problems relating to data, classification must be carried out, “according to who is the data holder and who is the data user, but also depend on the nature of data involved (personal data, non-personal data, or mixed data-sets combining the two)”²⁴⁹. Personal data can thus be classified according to so-called “data types”; the latter can

include data for commercial purposes or governmental purposes; data used by companies, including corporate data, human resources data, technical data and merchant data; instant and historic data; sensitive and non-sensitive data; and business-to-business (B2B), business-to-consumer (B2C), government-to-consumer (G2C) or consumer-to-consumer (C2C) data. Distinguishing among different types of data is important, because it may have implications on the kind of access that would need to be given to each type, both at national and international levels, as well as on how to handle the data. [...] These categorizations are important, as they might be the basis for differential treatment of data as they flow across borders. It may offer some potential insights for more granular regulation of cross-border data flows. However, given existing challenges in measuring and differentiating such flows, there may be limits to how these can be applied in practice. An important distinction is who the producers and consumers of data are. This implies exploring whether cross-border data flows are associated with B2B, G2C, B2C or C2C exchanges. It is also relevant to discuss additional cross-cutting issues, which may involve different treatment of data related to personal and sensitive data.²⁵⁰

An “information” is a central element of data. The term “information” is used inconsistently in law. Definitions differ between various disciplines, e.g., properties of information (indivisibility, irreversibility), their effects (inform, ability to differentiate, surprise), their dimensions (information as a process, content, or state) and conceptual

²⁴⁷ Aaronson, S.A. [Susan Ariell]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 7.

²⁴⁸ Steinrötter, B. [Björn]. (2020). Legal Framework for Commercialization of Digital Data. In M. [Martin] Ebers and S. [Susana] Navas (eds.), *Algorithms and Law* (pp. 269–298). Cambridge University Press. P. 272–273. P. 294

²⁴⁹ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 6.

²⁵⁰ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 78.

levels (syntactic, semantic, pragmatic). “Data” contain information that is recorded in such a way that it can be used or passed on. The term “data” has been used since the second half of the 20th century for information that is determined by measurements, observations and collections that is often digitally coded for machine storage and evaluation. Duplication of data is possible as well as simultaneous use by several individuals and their exclusivity is achieved through factual conditions, although data are basically of non-competing nature. All these criteria are different from physical objects. Ownership and property of the latter is possible, which led to a regulatory gap and therefore the interesting discourse if this could justify the creation of an absolute right for data.²⁵¹

Because there is no longer irrelevant data due to the development of information technology, personal data are to be defined widely, but not to be overstretched and be kept in mind that the objective, and also research focus of this thesis, is to protect the fundamental rights and freedoms of individuals, in particular their right to data protection with regard to the processing of personal data.²⁵² Data being personal falls in scope of the protection within the meaning of Arts. 7 and 8 of the Charter, whilst non-personal data do not have impacts on the fundamental rights of a natural person. This also makes it clear that data relating to legal persons are generally not protected.

Art. 2(a) Directive 95/46 and Art. 4(1) GDPR define personal data as any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person. Recital 30 GDPR determines that “cookies” are also considered personal data, while Recital 26 GDPR excludes “anonymized data” (“information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable”).

In other legal frameworks, “personal information” is the term more often in use. Another term but with similar meaning was introduced by the US through the federal “Privacy Act of 1974”²⁵³, wherein these data are called “personally identifiable information” (PII); and by the UN, which also spoke of “personally identifiable information”, which

may bear an (a) authorship in relation to the individual; (b) a descriptive relation to the individual; or (c) an instrumental mapping in relation to the individual. It is these aspects that may require protection from disclosure. Natural persons are ordinarily associated with personally identifiable information. In some States, legal persons and other entities may be affected. The scope of the topic *ratione personae* would have to determine the treatment to be given to other entities other than natural persons.²⁵⁴

²⁵¹ See below Chapter VIII, Section II.

²⁵² WP29. *Opinion 4/2007 on the concept of personal data*, WP 136, (2007). P. 25.

²⁵³ USA. *The Privacy Act of 1974*, Public Law No. 93-579, 5 U.S.C. § 552 a.

²⁵⁴ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 18.

5.2. Data Processing

The term “data processing” is not defined in the US framework, neither it is in both²⁵⁵ OECD Guidelines. Data processing shall be understood in this thesis as defined in Art. 4(2) GDPR as

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The definition in this thesis encompasses – unless otherwise noted – all “data processing steps” from the collection to the final erasure or destruction of personal data. Various “actors” are involved in these processing steps, which

may include Governments, intergovernmental organizations, non-governmental organizations and the private sector, such as multinational corporations and enterprises, some of which provide data processing services. The span of activities in the public or private sector that may be involved would have to be taken into account in the treatment of the topic.²⁵⁶

“Data controller” shall be understood as defined in Art. 4(7) GDPR, meaning “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.” “Processor” shall be understood as defined in Art. 4(8) GDPR, meaning “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.” “Recipient” shall be understood as defined in Art. 4(9) GDPR, meaning “a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.” “Third party” means a “natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.”, Art. 4(10) GDPR. Both controller and processor are “those responsible for a transfer”.

Controller or processor can be transferring personal data to another party in a “third country” and are in this case “data exporter”, whilst the controller or processor receiving the personal data are “data importer”. The GDPR’s principle of accountability, which is necessary to ensure the effective application of the level of protection, also applies to data transfers to third countries since those transfers fall below “data processing”.²⁵⁷

²⁵⁵ “Both” refers to the OECD Guidelines 1980 and the “*Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*”, C(80)58/FINAL, (11 July 2013), <https://www.oecd.org/sti/economy/2013-oecd-privacy-guidelines.pdf>, (“OECD Guidelines 2013”).

²⁵⁶ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 19.

²⁵⁷ EDPB (EDPB). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0*, (18 June 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf. Para 4. (“EDPB Recommendations 01/2020 (Version 2.0)”). // See also Schrems I. Para. 45

5.3. Transborder flow

The main medium for TFPD nowadays is the Internet. “Internet” is to be understood as a global network of networks that enables worldwide communication using a common protocol. “The Internet” consists therefore of different, interconnected networks. The Internet is decentralized, there is no “network center”, but a multitude of individual networks that together form the Internet. So, if computer A wants to transfer data over the Internet to computer B, which is connected to the Internet via an ISP, this data goes through different networks on the Internet. Internet users in their function as data subjects generally do not notice these different networks and the transfer via them but can make these transfer paths visible and understandable by using tools. An interplay of participants in those transfers can be private persons, businesses, as well as public institutions.

The notion of “the international circulation of information” was suggested by the French as more clearly reflecting the three characteristics involved: the automatic processing, information content, and electronic transmission. The essential elements recognized by those planning data flow activities were (1) the multi-country nature; (2) the content; and (3) the carriage dimensions, although it was felt that “international” was not the appropriate term because what actually occurs is the crossing of national borders, or frontiers.²⁵⁸ This definition appeared later in both the OECD Guidelines 1980 and the OECD “Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data” (OECD Guidelines 2013)²⁵⁹ as “movements of personal data across national borders”²⁶⁰. This could imply TFPD to be understood in a bilateral sense, meaning a data flow from country A to country B (and back).²⁶¹ But these data could also be included in multiple onward transfers from country B to other countries. This was also recognized by Weber, who found that

not every movement which can potentially lead to data crossing a border necessarily fulfils the meaning of the term “transborder”: Generally, it is assumed that, apart from the point-to-point transmission between the sender and the receiver of data domiciled in two countries, all data flows involving global networks (such as social networks and cloud computing) are covered. However, simply uploading information to the Internet and making it publicly available does not constitute a “transborder” data flow.²⁶²

Recital 101 of the GDPR defines “international data transfers”²⁶³ as “flows of personal data to and from countries outside the Union and international organizations. Nevertheless, such a starting point is not always an inherent part of legal definitions

²⁵⁸ Pipe, R. [Russell]. (1984). International information policy: Evolution of transborder data flow issues. *Telematics*, 1(4), 409–418. P. 409.

²⁵⁹ OECD. *Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>, (11 July 2013). (“OECD Guidelines 2013”).

²⁶⁰ OECD. *The OECD Privacy Framework*, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (2013). P. 13. (“OECD Privacy Framework”). // *Nota bene*: The OECD Privacy Framework not only encompasses the OECD Guidelines 2013, but also other Guidelines and *Memoranda* related to TFPD, such as, e.g., an Original Explanatory Memorandum to the OECD Privacy Guidelines (1980).

²⁶¹ The OECD acknowledged that this “point-to-point” interpretation was justifiable at earlier times, by stating that “when the 1980 Guidelines were drafted, data flows largely constituted discrete point-to-point transmissions between businesses or governments. Today, data can be processed simultaneously in multiple locations dispersed for storage around the globe; re-combined instantaneously; and moved across borders by individuals carrying mobile devices”. OECD Privacy Framework. P. 29.

²⁶² Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130. P. 118.

²⁶³ Whenever “transfer” or “data transfer” is mentioned in this thesis, a TFPD is meant.

worldwide. A “transborder data flow” has a geographical starting point, in contrast to the term “international data flow”. We therefore prefer to align with Convention 108+ and use “transborder” instead of “international”.

Furthermore, the distinction from “cross-border” is relevant. The Cambridge Dictionary describes “cross-border” as “between different countries, or involving people from different countries”, which suggests a common border.²⁶⁴ Art. 4(23) GDPR speaks of “cross-border processing” but does not make the use of this term dependent on a common border; rather, the focus of the definition lies on two local points of processing in more than one Member State. The delimitation of whether the participating countries have a common border or not, is not uniformly used for “cross-border” (common national border) and “transborder” (no common national border).

For this thesis, “cross-border” shall therefore be understood in the sense of “transborder” and “data flow” as any movement or transfer of data from one place to another, regardless of the mechanism used. A physical shipping of data embodied in tangible support from one country to another could also constitute a transborder data flow. In practice, however, these situations are only anecdotal due to the technological possibilities nowadays; we will therefore focus on the electronic transfer of such data.

Various places in the GDPR also equate a “transfer” with a “disclosure”, e.g., Art. 48 GDPR.²⁶⁵ Therefore, cases of access or disclosure are also to be understood as “transborder flow”, although a “flow” in the narrower sense does not exist. It was also recognized in Art. 14 Convention 108+ that “a transborder data transfer occurs when personal data are disclosed or made available to a recipient subject to the jurisdiction of another State or international organization”²⁶⁶.

5.4. Privacy and Data Protection

In scope of this thesis will be only TFPD. Within TFPD there is nevertheless a distinction between privacy and data protection to be clarified.²⁶⁷ The problem of overlapping notions of privacy and data protection will not be the focus of this research project, but has nevertheless to be addressed, at least to some extent, when considering the scope of a future legal instrument on TFPD. The UN spoke of

the right to privacy as centuries-old provenance [which] has attained constitutional status and recognition in many jurisdictions, as well as in international binding and non-binding instruments. However, the right to privacy is not absolute and its parameters and penumbras are not always easy to fathom and delineate. From philosophical and analytical perspectives, privacy conjures a variety of possibilities and ideas which may fall into one or crosscut any of the following clusters: (a) spatial; (b) decisional; (c) informational; and (d) privacy of communications.²⁶⁸

“Privacy” is a fundamental right with a long history, whereas “data protection” first appeared in the OECD Guidelines 1980. Interests for privacy as a legal object to be

²⁶⁴ Cambridge Dictionary. (2023). *cross-border*. <https://dictionary.cambridge.org/dictionary/english/cross-border>.

²⁶⁵ See also EDPB Recommendation 01/2020 (Version 2.0), footnote 23: “remote access by an entity from a third country to data located in the EEA is also considered a transfer.”

²⁶⁶ CoE. *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS No. 223, (10 October 2018). Para. 178. (“Explanatory Report to Convention 108+”).

²⁶⁷ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 13.

²⁶⁸ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 13.

protected, which broadened the pure physical right for life and property, date back to 1890, when Warren / Brandeis described privacy as “the right to be let alone”²⁶⁹. Scientific interests on this matter increased in the 1960s and 1970s with the advent of information technology. The genesis of modern legislation in this area can be traced to the first data protection law in the world, enacted in the Land of Hesse in Germany in 1970.²⁷⁰ In the influential decision of the German Constitutional Court (“*Volkszählungsurteil*”) from 15 December 1983, a fundamental right to informational self-determination was established in Germany by arguing that the sphere of individual freedom must be measured against Art. 2(1) of the German Constitution (“*Grundgesetz*”)²⁷¹ and that this self-determination is linked to human dignity guaranteed in Art. 1(1) of the German Constitution.²⁷² The German Constitutional Court found that “in this respect, the fundamental right guarantees the power of the individual to determine in principle for himself the disclosure and use of his personal data. Restrictions on this right to informational self-determination are only permissible in the overriding general interest”²⁷³. Since then, in parallel to the technical evolution, a distinction between privacy and data protection has become more difficult. It is clear that the concept of data protection has its origins in the right to privacy, the rest of the scientific discourse could be described as both having a significant overlap (“twins, but not identical”²⁷⁴).

On the European side, in previous draft versions of the GDPR, the terms “privacy” and “data protection” were used partially mixed. The final version uses “data protection” and avoids “privacy”. Although both fundamental rights are related, they are not congruent. However, the rights and freedoms of natural persons frequently referred to in the GDPR include the right to privacy according to Art. 7 of the Charter; “privacy” can therefore be implicitly included. The distinction between privacy and data protection has been examined also in the light of the jurisprudence of the CJEU and the European Court of Human Rights (ECtHR).²⁷⁵ Privacy could be seen as a broader notion, while data protection law “seeks to give rights to individuals in how data identifying them or pertaining to them are processed, and to subject such processing to a defined set of safeguards”²⁷⁶. Others argued “that the material scope of application of the data protection rules – determined by what constitutes “personal data” and “personal data processing” – is broader than the concept of “privacy interference” which defines the scope of application of Art. 8(1) ECHR [European Convention on Human Rights]”²⁷⁷²⁷⁸.

For example, although privacy law might recognize the right of the data subject to ensure the erasure of his personal data in certain instances, it does not recognize

²⁶⁹ Brandeis, L. [Louis] and Warren, S. [Samuel]. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220. P. 195.

²⁷⁰ *Bundesland Hessen. Datenschutzgesetz, Gesetz- und Verordnungsblatt für das Land Hessen*, 1 Y 3228 A, 625–627, (12 October 1970).

²⁷¹ Federal Republic of Germany. *Constitution for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III*, classification number 100-1, Federal Law Gazette I p. 968, (28 June 2022).

²⁷² German Federal Constitutional Court. *Judgment of the First Senate of 15 December 1983*, 1 BvR 209/83, 1–215.

²⁷³ German Federal Constitutional Court. *Judgment of the First Senate of 15 December 1983*, 1 BvR 209/83, 1–215. Paras. 92, 95.

²⁷⁴ de Hert, P. [Paul] and Schreuders, E. [Eric]. (2001). *The Relevance of Convention 108. European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future*. https://cris.vub.be/ws/portalfiles/portal/37771545/pdh2001_es_the_relevance_of_convention_108_.pdf. P. 36.

²⁷⁵ Kokott, J. [Juliane] and Sobotta, C. [Christoph]. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), 222–228. // Tzanou, M. [Maria]. (2013). Data protection as a fundamental right next to privacy? ‘Reconstructing’ a not so new right. *International Data Privacy Law*, 3(2), 88–99. // van der Sloot, B. [Bart]. (2014). Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, 4(4), 307–325.

²⁷⁶ Kuner, C. [Christopher]. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25(4), 307–317. P. 310.

²⁷⁷ CoE. *European Convention on Human Rights*, CETS 005, (4 November 1950). (“ECHR”).

²⁷⁸ Lynskey, O. [Orla]. (2014). Deconstructing data protection: The “added-value” of a right to data protection in the eu legal order. *International and Comparative Law Quarterly*, 63(3), 569–597. P. 582.

anything akin to the right to be forgotten set out in the GDPR. [...] The objective of such a right [to be forgotten] is not to protect individual privacy; it must therefore serve a different, independent objective. In conclusion, when determining whether the protection offered by Art. 8 ECHR is coextensive to that offered by the right to data protection, it can be seen that the two differ in terms of scope and also the substantive protection they offer. Therefore, it is suggested that the rights to data protection and privacy are significantly overlapping yet distinct.²⁷⁹

From a US perspective, the definitional problems of the notion privacy and that of PII have been addressed in different works.²⁸⁰ The term “privacy” used in the US is not to be equated in terms of content and terminology with “data protection”. A “Right to Privacy” is understood more extensively in the US. Terminologically, the US terms “informational privacy” or “information privacy” come close to the term “data protection” used in Europe.

The UN had limited the scope of its study at the time and limited it to the “informational subset of privacy, which deals with the individual’s control over the processing of personal data, it would be necessary to take into account the rights that the data subject and users possess”.²⁸¹ The UN further declared its intention to

address the protection to be afforded to the means of communication, that is to say, those aspects of [...] the privacy of communications insofar as there is a connection in securing informational privacy: the security and privacy of mail, telephony, e-mail and other forms of ICTs. With improved technologies, the availability of information in the public domain challenges the traditional paradigm of privacy as one protecting one’s hidden world. Data security, location data and traffic data have become elements within the penumbra of protection. Data security goes to the physical security of the data, an effort that seeks to ensure that data are not destroyed or tampered with in the place where they are located. Data are also always in a state of flux and movement and easily found in the custody of third Parties. Where one is located (location data) and what is being sent to another (traffic data) are matters whose anonymity can no longer be guaranteed. The type and nature of protection to be given to the data – whether stationary or in traffic – are matters that would fall within the purview of the topic.²⁸²

This thesis will understand “privacy” as the family and domestic sphere of a person, which is not accessible without the person’s consent and in which the person concerned exercises his or her right to the free development of his or her personality without being disturbed by external influences. It should be noted that privacy does not refer exclusively to the domestic sphere but may also exist in public. Privacy can be broader than data protection because if not only concerns information but can also be about, for example, physical spaces and choices of individuals during their self-determination, without personal data involved. But privacy can also be narrower, because data protection can

²⁷⁹ Lynskey, O. [Orla]. (2014). Deconstructing data protection: The “added-value” of a right to data protection in the eu legal order. *International and Comparative Law Quarterly*, 63(3), 569–597. P. 587.

²⁸⁰ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. // Ohm, P. [Paul]. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, Vol. 57, 1701–1777. // Schwartz, P. [Paul]. (2011). Personenbezogene Daten aus internationaler Perspektive. *Zeitschrift für Datenschutz*, 2011(3), 97–98. // Schwartz, P. [Paul] and Solove, D. [Daniel]. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 86(6), 1814–1894.

²⁸¹ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 14.

²⁸² UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 16.

apply irrespectively of whether there is an interference with the “private sphere”;²⁸³ privacy can but does not have to be affected by the violation of the right to data protection at the same time. There may be cases in which the above-mentioned right to informational self-determination may be affected, but not in the context of the private sphere of a person. Even the “European Data Protection Supervisor” (EDPS), stated that “experts do not always agree on the finer points of these two rights” and in its contribution itself omits a precise delimitation, but limits itself to an explanation of each part. We, too, leave open a final decision on this question.

Another distinction is necessary, namely between data protection and data security. Data security becomes relevant in this thesis, similar to what the UN stated, when data security can support the protection of personal data. The GDPR and the principles of other regulatory instruments worldwide have taken this into account.²⁸⁴

5.5. Regulation

TFPD occur within a web of legal frameworks. Such a “framework” is composed of rules, rights and obligations of companies, governments, and citizens set forth in a system of legal documents. Such frameworks are based on a mixed structure of public sources (national law, supranational law and international law) as well as private and hybrid norm sources (standards, codes, general business conditions) of the law. These different forms of legal frameworks, understood as the entirety of the norms assigned to a legal subject, contain the manifestations of legal sources. Ultimately, this thesis aims to show a possibility for an international regulatory instrument for TFPD. Such an instrument would penetrate and influence national laws in a variety of ways, while national laws and practices would shape such instrument. This leads to a confusing array of terms connected with the relationship between international and national law: “transnational law,” “law of nations,” “international law,” “public international law,” “private international law,” “international custom,” “general principles of law,” “conventions,” “treaties,” “agreements.” The concept of regulation is to be widely understood for this thesis and not restricted to government control. Regulation can thus have a form of influencing behavior, which can also be non-binding and detached from a State. It is therefore necessary to define a set of legal instruments connected to the term “regulation” in the context of this thesis.

“Regulation” shall be differentiated functionally and territorially. Functionally, the law can be understood as a restriction on the free movement of data. Such restrictions arise from regulatory measures. On the other hand, the law may also allow data transfer through the establishment of clear rules. Territorially, regulation is found in a field of tension between national, supranational, and international rules. Domestic regulation can relate to a foreign country. Natural or legal persons outside the national territory can be subject to this regulatory measure and acts of (foreign) persons exercised abroad can also be aimed at. A so-called “extraterritoriality” refers to the competence of a State to make, apply, and enforce regulation in respect of persons, objects, or actions beyond its territory. Such competence may be exercised by way of prescription, adjudication, or enforcement.

International law includes international public law, international commercial law, international private law and international uniform law. The sources of international law

²⁸³ The following example might highlight this: Whenever a MNE uses a global intranet, the names of the employees, their position and availability in the organization are part of this data, thus personal data is processed. Nevertheless, these personal data are not processed in a private sphere context, but in an employer-employee relationship context.

²⁸⁴ See below Chapter IX, Section III.2.

are set out in Art. 38(1)(a)-(d) of the Statute of the ICJ. “International conventions”²⁸⁵ are agreements between two or more countries. “International custom”²⁸⁶ presupposes a sufficiently solidified practice in the international community and a corresponding legal conviction due to a sense of legal obligation. The principles laid down in Art. 2 of the UN Charter, such as sovereign equality of the States, good faith, the settlement of their international disputes by peaceful means, the prohibition of the use of force, and cooperation are considered international custom. “general principles of law” are overarching legal standards of “civilized nations”, by which one understands today predominantly all Member States of the UN. Those standards are, for instance, the promotion of human rights and self-determination of a people, strict limitation of the use of force against other States, strict prohibition of acquisition of territory of another State by means of force, the principle of non-intervention, and the equality of States. General principles of law are subsidiary to international conventions and international custom. Art. 38(1)(d) of the Statute of the ICJ mentions another source of international law, which concerns instruments that are helpful in recognizing the shape of the sources of law. Art. 59 of the Statute of the ICJ states that the judgments of the ICJ are binding only between the disputing states, i.e., they apply *inter partes*. The international jurisprudence tends towards a functional-evaluative approach: General principles of law are not what the majority of legal systems agree on, but what turns out to be the best solution in a critical analysis of the solutions that emerge after a comparative legal survey. The respective legal principle must therefore be transposable to the international level so that this legal comparison becomes possible. Furthermore, the general principles of the law must not be a matter of pure equity considerations, as these are regulated in Art. 38(2) of the Statute of the ICJ.

International commercial customs, which are summarized in the term “*lex mercatoria*”, also have points of contact with the general principles of law. *Lex mercatoria* is usually broad and is intended to encompass all trade rules, including national and international law.²⁸⁷ The *lex mercatoria* therefore develops in the space between national law, supranational law, and international law, and has a habitual and direct origin in the private autonomy of those involved in world trade, the “*societas mercatorum*”.

International law may restrict the freedom of States to adopt measures concerning TFPD and it may seek to harmonize such measures, especially where contradictory requirements constitute an obstacle for international trade. The authority to set rules in international law arises from the sovereignty of a State. German law, for example, has adopted the *Grundgesetz* due to its constitutional power. This constitutional power is recognized by international law. Therefore, subjects of international law were and are primarily the States. Other international law subjects include international organizations and individuals in areas such as human rights protection. The international community of States, which participates in the event of a TFPD, can take different forms of connection, for example on the basis of a bilateral or multilateral agreements.

The end points of TFPD are subject to national jurisdiction, which has an impact on corresponding regulatory measures. National law may require such flows to take place in a certain manner and may restrict them. The construct of a State is the institutional consolidation of the territorially defined self-determination of a political community. It has a domain recognized by international law through territorial, personnel and flag sovereignty. The State in its connections to extraterritorial areas has also changed in the

²⁸⁵ Or also: “international agreements”, “international treaties”

²⁸⁶ Or also: “customary international law”

²⁸⁷ Lando, O. [Ole]. (1992). Principles of European Contract Law - An Alternative or a Precursor of European Legislation. *RabelsZ*, Vol. 56 (1992), 261 ff. P. 266.

course of time. Today it no longer exists only in relation to other countries, but also to international organizations and other legal entities.

“Supranational law” is a form of international law. It is based on the voluntary surrender of sovereignty of a State in favor of a higher level. European Union law is the prime example of a supranational legal framework. In the nature of its cooperation, the EU forms a special model without a prior historical model. In many fields, EU Member State law and EU law are so interwoven that it is no longer possible to make a clear distinction between the two. This is not the case in any other region of the world. One reason may be that this process encounters diverse political and cultural resistances on a global level, so that the internationalization of law can hardly keep pace with the globalization of its regulatory areas.

New forms of co-regulation between States and actors of the international, economic, and civil society can be observed today in various areas of society. However, the legal character of a system based outside the State is controversial. The ability to create justice is generally only granted to the State but not to private actors. By contrast, the existence of such “transnational law” is affirmed by representatives of legal pluralism. Transnational law is, according to Philip C. Jessup – former Justice of the ICJ – “law which regulates actions or events that transcend national frontiers. Both public and private international law are included, as are other rules which do not wholly fit into such standard categories”.²⁸⁸

Transnational law is then to be understood as law that (1) affects transborder, if not necessarily global, facts, (2) regulates both the relationships between individuals and objects of general interest, whereby it is regularly limited to individual subject areas, and (3) is predominantly, if not exclusively, contracted by non-State actors. It is supplemented by general legal principles that most legal systems contain. It achieves a relative independence from other legal systems through the establishment of its own dispute resolution mechanisms.²⁸⁹ In the literature, such transnational “norm aggregate” is also referred to as “hybrid regulations”²⁹⁰, “rules of governance”²⁹¹, “global constitution”²⁹², “global legal pluralism”²⁹³, “interlegality”²⁹⁴, “legal networks”²⁹⁵, or “regime collision norms”²⁹⁶; all of these should be synonymous with the term “transnational law” in this thesis. Transnational law is emerging as a new autonomous legal form beyond national law, supranational law, and international law. At the same time, these legal systems are interwoven in a variety of ways in such a way that the legitimacy of the law can only be guaranteed through their interaction.²⁹⁷ For the purpose of this thesis it is preferable to understand transnational law as a term alongside national, supranational, and international law, which cannot be assigned to either of these and is therefore, in contrast to territorially and hierarchically organized national, supranational, and international law,

²⁸⁸ Jessup, P. [Philip]. (1956). *Transnational Law*. Yale University Press. P. 1.

²⁸⁹ Viellechner, L. [Lars]. (2013). *Transnationalisierung des Rechts*. Velbrück. P. 180 f.

²⁹⁰ Sand, I.-J. [Inger-Johanne]. (2009). Hybrid Law: Law in a Global Society of Differentiation and Change. In G.-P. [Gralf-Peter] Callies and A. [Andreas] Fischer-Lescano and D. [Dan] Wielsch and P. [Peer] Zumbansen, *Soziologische Jurisprudenz: Festschrift für Gunther Teubner zum 65. Geburtstag (871–886)*. De Gruyter.

²⁹¹ Walker, N. [Neil]. (2008). Beyond Boundary Disputes and Basic Grids: Mapping the Global Disorder of Normative Orders. *International Journal of Constitutional Law*, 6(3-4), 373–396.

²⁹² Fischer-Lescano, A. [Andreas]. (2005). *Globalverfassung: Die Geltungsbegründung der Menschenrechte*. Velbrück.

²⁹³ Schiff Berman, P. [Paul]. (2012). *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders*. Cambridge University Press.

²⁹⁴ Amstutz, M. [Marc]. (2005). In-Between Worlds: Marleasing and the Emergence of Interlegality in Legal Reasoning. *European Law Journal*, 11(6), 766–784.

²⁹⁵ Ladeur, K.-H. [Karl-Heinz]. (2011). Ein Recht der Netzwerke für die Weltgesellschaft oder Konstitutionalisierung der Völkergemeinschaft?. *Archiv des Völkerrechts*, 49(3), 246–275.

²⁹⁶ Fischer-Lescano, A. [Andreas] and Teubner, G. [Gunther]. (2006). *Regime-Kollisionen: Zur Fragmentierung des globalen Rechts*. Suhrkamp.

²⁹⁷ Viellechner, L. [Lars]. (2013). *Transnationalisierung des Rechts*. Velbrück. P. 11.

fragmented into a multitude of functional, specialized legal regimes that pragmatically combine institutions of both private and State origin. Transnational law is nevertheless not indefinitely self-supporting but should have consistent basic values as a criterion when assessing conflicts of interest. This would require basic values that are shared by many national laws. However, this does not yet lead to the existence of an autonomous legal system, but only to the recognition of these basic values either by national law, supranational law, or by international law. In practice, the recognition of a transnational law for this thesis could mean, for example, that principles in a contract for data processing, which two companies subject to international trade law, could become effective if a national judge recognizes these principles as transnationally valid.

Related to other non-legislative measures, there is a discussion in international law about the existence of so-called “soft law”. Abbott and Snidal found that

hard law refers to legally binding obligations that are precise (or can be made precise through adjudication or the issuance of detailed regulations) and that delegate authority for interpreting and implementing the law. [...] The realm of soft law begins once legal arrangements are weakened along one or more of the dimensions of obligation, precision, and delegation. This softening can occur in varying degrees along each dimension and in different combinations across dimensions. We use the shorthand term soft law to distinguish this broad class of deviations from hard law – and, at the other extreme, from purely political arrangements in which legalization is largely absent. But bear in mind that soft law comes in many varieties: the choice between hard law and soft law is not a binary one.²⁹⁸

Some see resolutions of the UN General Assembly, that are important for the development of human rights, also as soft law.²⁹⁹ Nevertheless, caution is required, because either something is law, then it is binding, or it is simply not yet law. Even if soft law is used to confirm existing legal propositions, such as the General Assembly resolutions, although it does not strengthen the law, contributes to the establishment of law from other sources. The necessity of the category of soft law can therefore not entirely be doubted.

International law regards some rights as so significant that they are declared mandatory (“*ius cogens*”). Those concern the most flagrant violations of human dignity, genocide, and crimes against humanity. The peculiarity of this category of law is that even unilateral actions or declarations of States cannot absolve them from the applicability of *ius cogens*. In a hierarchy of norms, *ius cogens* is at the top, and it cannot – unlike “*ius dispositivum*” – be deviated from it. It can only be supplanted by equals of the same rank, that is, competing *ius cogens*. The concept of *ius cogens* and this hierarchy in international law is recognized by the “Vienna Convention on the Law of Treaties” (VCLT)³⁰⁰.

“Self-regulation” is characterized by the fact that systems are regulated with the participation of the systems themselves and not solely by outsiders. It is questionable whether self-regulation relates to private interests and / or public interests. In part, self-regulation is understood as the individual or collective pursuit of private interests in the

²⁹⁸ Abbott, K. W. [Kenneth Wayne] and Snidal, D. [Duncan]. (2000). Hard and Soft Law in International Governance. *International Organization*, 54(3), 421–456. P. 421–422.

²⁹⁹ Dupuy, P.-M. [Pierre-Marie]. (1991). Soft Law and the International Law of the Environment. *Michigan Journal of International Law*, 12(2), 420–435. P. 422. // Barelli, M. [Mauro]. The Role of Soft Law in the International Legal System: The Case of the United Nations Declaration on the Rights of Indigenous Peoples. *International & Comparative Law Quarterly*, 58(4), 957–983. P. 958 f.

³⁰⁰ UN. *Vienna Convention on the Law of Treaties*, United Nations Treaty Series, vol. 1155, P. 331 ff., (1969). (“VCLT”)

exercise of fundamental rights to legitimate self-interest.³⁰¹ A definition based on the pursuit of interests, however, narrows the concept of self-regulation and, with a variety of motivations, brings with it the challenge of evaluation of interests pursued in the specific case. Since private and public interests are not always easy to separate, this distinction can be difficult in individual cases. It is therefore preferable to use one of the definition approaches that does not focus (only) on the interests pursued by the regulation. Some consider the autonomy of the rule-setters to be crucial; according to them, self-regulation is the voluntary regulation of their own behavior and the formation of collective orders by a non-governmental body.³⁰² This definition is too narrow since it does not necessarily cover regulatory participation by a State. A term that relates to the essential element of self-regulation, namely the integration of private and public law regulation, is therefore preferable. For the further course of this thesis, and with Bachmann³⁰³, self-regulation is understood as the area of social life that for certain reasons is not left to the free play of market forces, and for other reasons it is not to be directly assigned to a State. Ultimately, the question of the legal definition of a data protection system that is developing through self-regulation cannot be analyzed entirely as part of this thesis. The question as to whether genuine law arises from self-regulatory measures in data protection will accordingly be left open.

5.6. Jurisdiction

The territorial context of TFPD is often unclear, which makes it difficult to trace whether a TFPD has taken place or whether the data were processed by domestic servers only. The nationality of the data subject and the country of origin of personal data have become practically irrelevant for the determination of the processing location. The connection between ubiquity and virtuality of activities including the processing of personal data led to an almost unlimited number of governmental and non-governmental databases and those responsible for such TFPD.

In international law, the term “jurisdiction” relates to the “sovereignty” of the State, including everything that is within its national territory, as well as all citizens of this State outside the national territory. While “sovereignty” comprises, among other things, the autonomy of a State as well as its independence from other States under international law, the concept of jurisdiction describes the concrete exercise of power by the individual State based on its sovereignty.

It is important to distinguish applicable law and jurisdiction in the context of data protection because these could otherwise be concepts to be easily confused in this thesis. Kuner noted justifiably in this respect that

jurisdiction under public international law is generally defined as the State’s right under international law to regulate conduct in matters not exclusively of domestic concern, and is contrasted with choice of law, conflict of laws, or applicable law, which deal with the question of which law or laws shall be applied in a given case. However, jurisdiction and choice of law are closely related, and the distinction between the two terms, if it ever was clear, has become increasingly vague. [...] In practice, national data protection authorities often equate jurisdiction and choice of law.³⁰⁴

³⁰¹ Calliess, C. [Christian]. (2002). Inhalt, Dogmatik und Grenzen der Selbstregulierung im Medienrecht, *AfP* 2002(6), 465–475. P. 466.

³⁰² Hoeren, T. [Thomas]. (1995). *Selbstregulierung im Banken- und Versicherungsrecht*. Verlag Versicherungswirtschaft. P. 5 f.

³⁰³ Bachmann, G. [Gregor]. (2006). *Private Ordnung*. Mohr Siebeck. P. 27.

³⁰⁴ Kuner, C. [Christopher]. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 1). *International Journal of Law and Information Technology*, 18(2), 176–193. P. 178–180.

Directive 95/46 confirms this risk of equation also, if one looks at the interaction between Art. 4 Directive 95/46 (header “national law applicable”) and Art. 28(6) Directive 95/46 (jurisdictional considerations, but only for the cooperation of SAs).

International law coordinates the national legal systems and allocates regulatory powers. It fulfills the function of a superordinate “conflict of laws”. Conflict of laws rules are then put into concrete terms by the States in their national conflict of laws ruleset. This ruleset is usually meant when it is referred to “Private International Law” (PIL). International law only lays down a minimum standard and – unlike PIL – does not pursue the goal of determining the most appropriate legal system for a particular set of circumstances. Although this thesis is not purely PIL-related, it is nevertheless necessary to present principles of PIL. PIL starts with qualification, the subsumption of the facts under a conflict of law rule, and the question of how the terms in question are to be interpreted to ultimately understand a legal norm unknown to domestic law (e.g., for German law the Islamic morning gift). An “*ordre public*”³⁰⁵ is the essence of domestic values. Only when, through comparison with a corresponding domestic norm, it has been found that the application of a foreign norm, to which, e.g., the German PIL refers to, “essentially” violates such domestic values, the foreign law can exceptionally be ignored for the solution of the specific legal issue (in German law according to Art. 6 “*Einführungsgesetz zum Bürgerlichen Gesetzbuche*” (EGBGB)³⁰⁶. The situation is similar with “substitution”. The question here is whether a foreign legal norm is so equivalent to a domestic one that it can replace the latter. Likewise, in the doctrine of a so-called “*renvoi*”, the question of whether the acceptance or rejection of a foreign referral norm that is based on domestic law leads to the harmony of decisions aimed at by IPL, can only be coped with comparative law.

For jurisdiction in international law, especially in English-speaking countries, a division is made between the “jurisdiction to prescribe”, the “jurisdiction to adjudicate”, and the “jurisdiction to enforce”. This division follows the traditional division of a State’s authority between legislation, judicial and enforcement powers, whilst each branch of government can theoretically engage in any of the three. Therefore, these jurisdictions do not necessarily have to coincide. This becomes clear when a State attempts to represent its interests outside its national territory by regulating matters that have a connection to another State. As TFPD are such a matter, a definition becomes important to this thesis. Jurisdiction to prescribe concerns the question of whether a State is permitted to regulate an issue; regulation hereby means not only the issuing of general legal sentences, but also the issuing of administrative acts or judgments. Jurisdiction to adjudicate is a State’s ability to subject persons or things to the process of its courts or administrative tribunals. Jurisdiction to enforce deals with the physical aspect of the exercise of sovereignty, such as the execution of an administrative act. In the context of the present work, if not stated otherwise, sovereignty is understood in the sense of the jurisdiction to prescribe.

The distinction between the jurisdiction to prescribe and the jurisdiction to enforce can be explained exemplarily with the *LICRA v. Yahoo* case. The case concerned an auction offered via Yahoo, in which Nazi memorabilia were for sale via the Internet. The French court prohibited Yahoo, under French law, from making the offer available in France. In the US, the offer was protected by fundamental right of freedom of expression. Yahoo won a judgment in the US that enforcement of French judgments in the US would violate the First Amendment of the US Constitution.³⁰⁷ Yahoo then agreed with France and largely ruled out technical measures to prevent French users from accessing the relevant

³⁰⁵ Or “public policy”, the common law counterpart.

³⁰⁶ Federal Republic of Germany. *Introductory Act to the German Civil Code*, BGBl. I p. 3515, (10 August 2021). (“EGBGB”).

³⁰⁷ *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L’Antisémitisme*, 145 F. Supp.2d 1168, 1180 (N.D. Cal. 2001)

webpage. It is part of the principle of territoriality in the area of jurisdiction to prescribe that France can impose a distribution ban on access from its territory. France can hereby not be prevented from doing by the protection of fundamental rights in the US for the offer made on American territory. Conversely, France cannot force the US to participate in the enforcement of its decisions in the US.

Regulatory sovereignty is not exclusive and, depending on the circumstances, more than one State can be granted authorization. The sovereignty of a State sets the limits for the jurisdictional reach of other States; they are committed to each other to maintain their sovereignty. Sovereignty can be delimited by international law. A State can therefore theoretically act (prescribe, adjudicate, as well as enforce) on foreign territory if there is a basis for authorization under international law. In TFPD scenarios, national regulations are often applied across borders. These cases then represent a so-called “extraterritorial prescriptive jurisdiction”. In these scenarios, a national legal norm regulates matters with foreign implications, i.e., its material scope extends beyond the own national territory and thus has a so-called “extraterritorial effect”. These scenarios are therefore particularly susceptible to an extension of national regulations, so that such forms of data processing activities may be exposed to several national and possibly even conflicting regulations. As will be shown in more detail below³⁰⁸, this can lead to international conflict situations.

III. Conclusive remarks

As shown above, the state of the art of TFPD changed significantly in the last five decades. While there was previously a geographical link between data processing and the country of origin of the data, it has practically dissolved due to the development of the Internet and the globalization of the digital economy. The internationalized processing of personal data has become the norm due to the connection of computers and telecommunication networks made possible by the Internet. As a result of global networking, transborder data traffic is no longer a deliberate decision made by the individual user, but often the result of server capacities at the disposal of a SP. This creates virtualized data processing, which is carried out simultaneously within a worldwide distributed network of servers.

As a result, the territorial context of this data processing is often unclear, which makes it difficult to trace whether a TFPD has taken place or whether the data were processed by domestic servers only. The nationality of the data subject and the country of origin of the data have become practically irrelevant for the determination of the processing location. The connection between ubiquity and virtuality of access to personal data led to an almost unlimited number of governmental and non-governmental databases and data controllers.

From an economic perspective, data has become an important raw material for the global economy. They are considered “the new oil”. TFPD have become a necessary part of modern, globalized societies and of great economic importance. My colleague Kulhari at the Max-Planck-Institute for Innovation and Competition in Munich stated accordingly in her preliminary findings that “varying standards of data protection highlight existing divergence on the global stage and act as deterrent to international trade”³⁰⁹. We agree with her that “responsible use and processing of personal data is at the forefront of extracting the “good” from data” and that “this makes data protection a desirable legal

³⁰⁸ Chapter VIII, Section III.

³⁰⁹ Kulhari, S. [Shraddha]. (2023). *Global Convergence of Data Protection Norms: An Agenda for Development & Trade*. Poster, Max Planck Institute for Innovation and Competition, Munich.

tool”.³¹⁰ However, we are not convinced that “a trade-based solution seems to be the most palpable in order to build momentum towards the global convergence of data protection frameworks on the basis of minimum standards”³¹¹. We stand for minimum standards yes, but based on a human-centric approach³¹² grounded in fundamental rights.

In this context, companies therefore have only a minor interest in restrictive data protection legislation.³¹³ The transfer of data collected for the purpose of commercial “exploitation” from one legal system to the next has certainly facilitated this.

From a data subjects’ point of view, the main problem could be that adequate data protection is not guaranteed in every scenario of a TFPD. The technical development has led to expanded usage of options which are mostly no longer manageable by the data subjects. The internationalized and location-flexible data processing associated with the development of, e.g., cloud computing, means that the control of data once sent could be less effective abroad, as detection and prevention of abuse are increasingly difficult. At the latest, since the NSA affair, there has been public awareness of the risks of this development. Without ensuring data protection levels for TFPD there could be the risk of data subjects experiencing a feeling of powerlessness and resignation and thus a loss of trust in the legal system as such. Protecting the right to privacy and personal data has become central to the further development of a development-oriented and people-centered information society. A lack of trust in a protected private sphere could undermine the central participatory rights in the information society with the freedom of communication. To achieve this, all relevant stakeholders must be able to participate in the development of rules. This presupposes models for the democratic legitimation of Internet governance standards and poses major challenges for classic international law.

This accelerates the need to answer questions of the digitization of everything. This digital transformation has implications for the global digital economy, especially the transatlantic EU-US relationship, considering the differences that have developed concerning the appropriate balance between personal data protection, economic growth and (national) security. Data protection became an essential value of the EU-US information society. In late November 2020, Adam Klein, chair of the U.S. government’s Privacy and Civil Liberties Oversight Board (PCLOB) noted correspondingly:

Transatlantic discussions about surveillance and privacy could be improved by greater candor about what each side is doing, and why. Ultimately, Americans and Europeans face the same challenge: protecting our societies in a manner consistent with fundamental values and the rule of law. Respectful, candid discussion of these issues can help both sides do that better.³¹⁴

Because of the rapid development within the dimensions “Technology”, “Economy”, “Sociology” and “Policy” described above, the question of the impact on an international regulation of this area of law arises. We agree with Trakman / Walters / Zeller who, regarding the interplay between these four dimensions, argue that

³¹⁰ Kulhari, S. [Shraddha]. (2023). *Global Convergence of Data Protection Norms: An Agenda for Development & Trade*. Poster, Max Planck Institute for Innovation and Competition, Munich.

³¹¹ Kulhari, S. [Shraddha]. (2023). *Global Convergence of Data Protection Norms: An Agenda for Development & Trade*. Poster, Max Planck Institute for Innovation and Competition, Munich.

³¹² See also below Chapter IX, Section I.

³¹³ See also below Chapter X, Section II.3.

³¹⁴ US Privacy and Civil Liberties Oversight Board. (2020). *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*. https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf. P. 4.

a further policy consideration is to acknowledge that, while individual states or associations of states such as in the EU, can protect personal data domestically, it is difficult for a multiplicity of states with different economic, social and political agendas to regulate personal data similarly. It is also challenging for them to address the constantly changing internationalization of the Internet and its infrastructure. On the one hand, nation states have not kept pace with global technological developments. Concentrating primarily on their distinct sovereign needs, they have engaged in ad hoc and inconsistent approaches to protecting personal data.³¹⁵

Similarly, Birgitta Jónsdóttir, a former Icelandic politician and then a prominent Wikileaks supporter, said that “as a matter of fact no legislator in the world has been able to keep up with that development”.³¹⁶ All dimensions mentioned in Chapter I Section I are closely related. Technological progress has enabled economic growth that also depends on a free TFPD, in particular between the G20 countries. This flow has also gained importance on the social level, mainly as a result of the rapid increase in use of social media. Consequently, data protection as an aspect of the protection of privacy has also become a focus of policy. For agreements with trading partners of the EU, a sort of “blueprint” had already been created by Safe Harbor and Privacy Shield.

Schrems II brought with it the need to react again to a new legal situation. The EU Commission’s adequacy decision relating to Privacy Shield was annulled. Data transfers to third countries can no longer be based on Privacy Shield. Data transfers on the basis of SDPC remain possible, under the GDPR, provided that the guarantees contained therein are sufficient to establish an essentially equivalent level of protection with a view to the legal situation in the recipient country. This assessment with regard to the creation of such level of protection can be transferred to the other guarantees set out in Art. 46 GDPR (in particular BCR and “Codes of Conduct” (CoC)). If there is no alternative legal basis for the legitimation of data transfers, those responsible for the TFPD have to assess whether data protection concerns can be overcome by “supplementary measures”³¹⁷ such as technical measures (e.g., anonymization or pseudonymization, encryption technologies). Those responsible must promptly identify the relevant data transfers with reference to third countries, make appropriate documentation and make a (risk) decision on further action based on reliable information. In the aftermath of *Schrems II*, the Commission issued new sets of SDPC and the “European Data Protection Board” (EDPB) published several recommendations on the matter. These publications came in a rapid succession, quite unusually for the Commission and the EDPB. There was great concern of regulators about legal certainty and the digital economy’s resulting reaction to the annulment of the Commission’s adequacy decision on Privacy Shield. It remains to be seen whether and to what extent a possible Privacy Shield 2.0 could be a model for agreements with third countries. In any case, this would not be more than just another bilateral patchwork and would not lead to a sustainable solution.

³¹⁵ Trakman, L. [Leon] and Walters, R. [Robert] and Zeller, B. [Bruno]. (2019). Is Privacy and Personal Data Set to Become the New Intellectual Property?. *International Review of Intellectual Property and Competition Law*, 937–970, <http://dx.doi.org/10.2139/ssrn.3448959>. P. 944.

³¹⁶ Jónsdóttir, B. [Birgitta]. (8 May 2016). *Being offline is the new luxury*. Netherlands Public Broadcasting (NPO), VPRO Documentary. <https://www.vpro.nl/programmas/tegenlicht/kijk/backlight/Offline-is-the-new-luxury.html>.

³¹⁷ At this point, reference must be made to *termini tecnici* that may be confusing for the reader. “Supplementary measures” (definition of the EDPB) is in this thesis synonymous with “additional measures” (definition of the Commission and the OECD). We follow the definition of the EDPB in order not to confuse the reader with the proximity to “additional safeguards” (Directive 95/46).

FIRST PART: THE CURRENT WORLDWIDE REGULATORY MOSAIC

The relevance of TFPD as well as the need for international harmonization of such flows have been outlined in the INTRODUCTORY PART (Chapter I). However, the obstacles are still substantial and, in practice, demands for substantial harmonization at the international level have remained largely unsuccessful. Ultimately, a binding, comprehensive “world data protection law” appears to be necessary but so far has proven politically elusive.

The “dimensions” above³¹⁸ showed that rapid technological progress is often unpredictable and brings about effects in the other three dimensions. The newer technologies are used in a modern society, the more difficult it becomes to control those effects. As a result, new social and legal challenges appear, which legislators must work on and properly assess against the social background.

These challenges give rise to regulatory uncertainty for States, and fears of their loss of sovereignty, as States’ viewpoint on data protection in general – and on TFPD in particular – as well as their understanding of the role of the State in this are often too different.³¹⁹

In this FIRST PART we will present the complex and colorful regulatory mosaic that affects today’s phenomenon of TFPD, focusing particularly on the US, the EU, the APAC, the relevant international organizations, as well as on self-regulatory approaches.

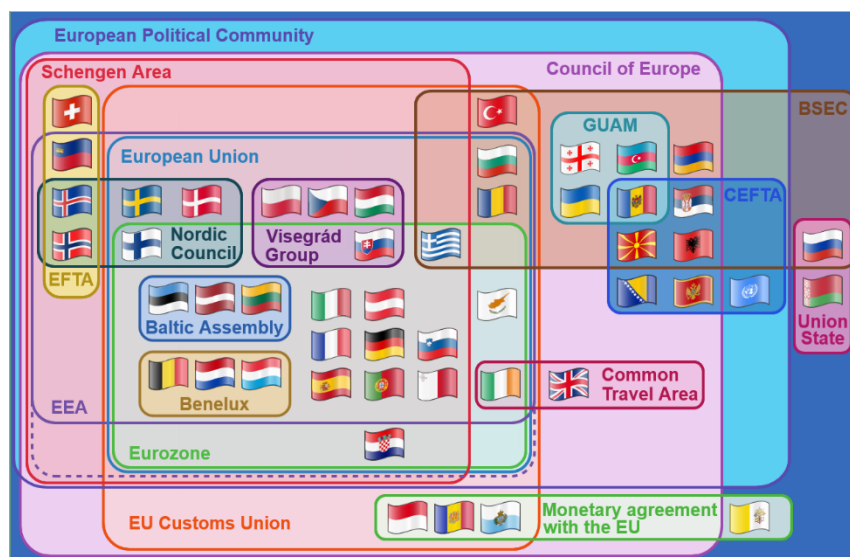
³¹⁸ Chapter I, Section I.

³¹⁹ Kuner, C. [Christopher]. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25(4), 307–317. P. 310 // Fischer, P. E. [Philipp Eberhard]. (2012). *Will Privacy Law in the 21st Century be American, European or International?* GRIN Verlag. <https://www.grin.com/document/187981>. P. 25.

CHAPTER II: EUROPEAN FRAMEWORK

I. Legislative bodies and their relationships

To understand the emergence of an instrument within the European framework, an overview of the complex interplay of bodies and their relations within this framework is relevant.



Source: Wikipedia, "Supranational European Bodies"³²⁰

The European framework is based upon regulatory instruments by the EU and CoE. The three institutions involved in EU legislation are the "European Parliament" (the "Parliament" or "EP"), the "Council of the European Union" (the "Council") and the Commission.

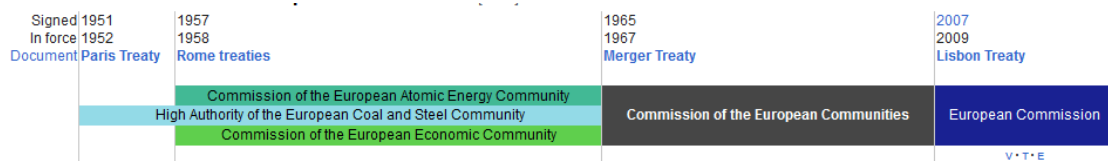
The Parliament is the legislative body of the EU. With over 700 members, it is directly elected every five years by the 500 million citizens of the Member States. The basis for the decision-making processes in the EU and the functioning of the institutions is determined by the citizens exercising their right to vote.

The Council represents the governments of Member States. The Presidency of the Council is shared by the Member States on a rotating basis. Led by the President of the Council and comprising national heads of State or government, it meets at least every 6 months. Most European laws are adopted jointly by the Parliament and the Council, in

³²⁰ Wikipedia. (5 March 2023). *Supranational European Bodies*.
https://en.wikipedia.org/wiki/File:Supranational_European_Bodies-en.svg.

what was known as the “co-decision procedure”.³²¹ With the “Treaty of Lisbon”³²², the co-decision procedure was renamed the “ordinary legislative procedure”. The Council is neither to be confused with the “European Council” (which arranges quarterly summits, where EU leaders meet to set the direction of EU policy making), nor with the CoE (not an EU body at all).

The European Commission is the executive of the EU. It is responsible for drawing up proposals for new European legislation and implementing the decisions of the Parliament and the Council. The Commission sets the EU’s overall political direction – but has no powers to pass legislation. It is important to note that the name of the Commission has changed over the years as it has evolved from EC to EU; in this thesis, both names are synonymous as “Commission”.



Source: Wikipedia, “Structural evolution of the European Commission”³²³

The CJEU upholds the rule of European law in its function as the supreme judicial body of the EU. It reviews the legality of the acts of the EU Institutions, ensures that Member States comply with obligations under the EU treaties and interprets EU law at the request of Member State courts.

The Heads of Government of the 27 Member States, as well as the Presidents of the Commission and of the CoE are part of the European Council. Whenever the media speaks of a “European Summit of Heads of State or Government”, they refer to the European Council. The European Council has the task of defining guidelines of the European policy, strategy for the further development of the EU, and urgent fields of action. At the end of its meetings, the European Council adopts conclusions with recommendations for action. However, the European Council itself is not entitled to pass legislation.

The CoE is an intergovernmental non-EU organization committed to democracy and human rights. It includes the “European Court of Human Rights” (ECtHR) in Strasbourg. The CoE had been founded through the Contract of London³²⁴. The CoE at present has 46³²⁵ Member States including non-EU countries such as, for example, Turkey. Although being different organizations that play different roles, the CoE and the EU are based on the same essential values: human rights, democracy, and the rule of law. The “Memorandum of Understanding between the Council of Europe and the European Union” underlines that both entities share priorities which also encompass aspects of

³²¹ Council of the EU. (2023). *The ordinary legislative procedure*. <https://www.consilium.europa.eu/en/council-eu/decision-making/ordinary-legislative-procedure>.

³²² EU. *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on European Union - Protocols - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon*, Official Journal of the European Union, C 326, 1–390, (signed on 13 December 2007, published 26 October 2012). (“Treaty of Lisbon”).

³²³ Wikipedia. (2023). *Structural evolution of the European Commission*. https://en.wikipedia.org/wiki/European_Communities.

³²⁴ CoE. *Statute of the Council of Europe*, ETS No. 001, (5 May 1949).

³²⁵ Russia has been excluded due to the war in Ukraine. // See CoE. (16 March 2022). *The Russian Federation is excluded from the Council of Europe*. <https://www.coe.int/en/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe>.

human rights and fundamental freedoms.³²⁶ The CoE places these essential values at the heart of its work and monitors the application of these standards by the countries that have signed the relevant contract. In addition, the CoE, often in cooperation with the EU, provides technical assistance to help countries meet their obligations. The EU identifies these “European values” as key elements for its political and economic integration process. The EU often relies upon the standards of the CoE for the creation of legal instruments and -agreements for its 27 Member States. The ECHR obliges the Member States but does not produce direct legal effect within the Member States’ national legal orders; this rather requires a national implementation.

Union law is a “supranational” legal framework *sui generis*. Since the Treaty of Lisbon, the correct term for it is “Union law”, while “Community law” is only of historical definition. EU data protection rules can apply to the EEA, which includes all EU countries plus the non-EU countries Iceland, Liechtenstein and Norway.³²⁷

II. Legislation of the EU

1. Union law system

Union law consists of primary and secondary legislation. According to the normative hierarchy of Union law, primary law prevails over all other sources of law. Secondary law must not be contrary to primary law. Lower-ranking law is to be interpreted in a constitutional manner. The CJEU is responsible for securing this primacy through a variety of forms of action, such as action for annulment and preliminary ruling. However, if the lower-ranking law is compatible with the higher-ranking law and the same legal consequences arise from both sources of law, the lower-ranking law must be applied because it is, in principle, more precise than the higher-ranking one.

Primary law encompasses the EU founding treaties in their amended versions. The Treaty of Lisbon entered into force on 1 December 2009. It amended the “Treaty of Maastricht”, known in its updated form as the “Treaty on the European Union” (TEU)³²⁸, and the “Treaty of Rome”, known in its updated form as the “Treaty on the Functioning of the European Union” (TFEU)³²⁹. It also amended the “Treaty Protocols” as well as the “Treaty establishing the European Atomic Energy Community” (EURATOM)³³⁰. The Treaty Protocols are regarded as legally equivalent to the TEU / TFEU provisions, “as part of the Treaties” (Art. 51 TEU). Primary law contains the basic rules on the functioning of the EU. The CJEU repeatedly referred to it as the “constitutional document of the Community” because of the functional similarity of primary law with national constitutions. There are no normative hierarchies within the treaties, all provisions are on the same hierarchical level, without a differentiation between more important and less important,

³²⁶ CoE. *Memorandum of Understanding between the Council of Europe and the European Union*, <https://rm.coe.int/1680597b32>, (23 May 2007). Para 19: “In the field of human rights and fundamental freedoms, coherence of the Community and European Union law with the relevant conventions of the Council of Europe will be ensured. This does not prevent Community and European Union law from providing more extensive protection.”

³²⁷ In order to apply to these EEA countries, legislation must be reviewed by the EEA Committee and, if it is to be applied, incorporated into the Protocols and Annexes to the “Agreement on the European Economic Area, OJ No L 1, 3 January 1994” (“EEA Agreement”). In the field of data protection, the EEA Agreement covers EU legislation of general application to commercial activities. Directive 95/46 had been incorporated into the EEA Agreement by 26 June 1999, but is no longer in force in the Agreement. For the GDPR, this revision was done on 6 July 2018, the GDPR is now directly applicable within the EEA as of 20 July 2018.

³²⁸ EU. *Consolidated version of the Treaty on European Union*, *Official Journal of the European Union*, C 326/13, (26 October 2012). (“TEU”).

³²⁹ EU. *Consolidated version of the Treaty on the Functioning of the European Union*, *Official Journal of the European Union*, C 326/47, (26 October 2012). (“TFEU”).

³³⁰ EU. *Consolidated version of the Treaty establishing the European Atomic Energy Community*, OJ C 327, 1–107, (26 October 2012). (“EURATOM”).

more general and concrete norms. The same applies to the provisions of the Protocols, Art. 311 TEU.

Primary law also consists of unwritten European law. This includes the so-called “general principles” of Union law, which are applied by the CJEU and the national courts of the Member States when determining the lawfulness of legislative and administrative measures within the Union. Of main importance at this point is the protection of fundamental rights developed and guaranteed by the Union’s jurisdiction. In addition to the fundamental rights as well as the fundamental procedural rights, these general principles are placed as superordinate interpretative measures in the rank of primary law. These guarantee the material legality of the Union and thus also the action of its Member States within the scope of Union Law. A rarer form of unwritten primary law is common law, which arises from constant practice (*consuetudo*) and corresponding legal conviction (*opinio iuris*). The limits to the development of the law are fluid in this respect.

All treaties of primary law have been ratified as international agreements. Nonetheless, Union law is not equal to international law and, in principle, supersedes the general rules of international law through more specific Union law in the EU. The core area of Union law has some special features that are not common in international law: Union citizens, for example, can directly claim their rights guaranteed by Union law before the courts of the Member States, whereas international law usually must be implemented in national law before citizens can invoke a court based on international law. Common international law binds the Union where there are no special arrangements in the Union, particularly in contractual external relations. There is an increased international cooperation from European side, which leads to the emergence of territorial “Europeanized” international law, because norms of international law can be at the same time part of EU law. The legal systems of the Member States are also determined by the international agreements of the EU itself. However, the international agreements of the EU do not bind the Member States under international law but are to be observed because of the binding nature of EU law. According to the CJEU, international agreements form an “integral part” of EU law insofar as the subject-matter of the treaty falls within the EU’s competence.³³¹ The CJEU therefore has jurisdiction to give preliminary rulings concerning the interpretation of such an agreement.³³² International agreements of the EU can have the same effects as other Union law. International law can thus also serve the purpose of supplementing the law of the Union. However, the Union remains bound by *ius cogens*, which cannot be circumvented by Union treaties.

Secondary law comprises acts adopted based on primary law by the institutions of the Union or EURATOM (Art. 288 TFEU). A “Regulation” is directly applicable and binding in all Member States. It does not have to be implemented by the Member States into national law. A “Directive” obliges the Member States or a group of Member States to achieve a specific result. Directives must be implemented into national law to be effective. In other words, a Directive sets out the objective, but it is up to the individual Member States to decide their way to achieve it. A “Decision” may be addressed to Member States, groups, or individuals. It is binding in all its parts. Decisions are made, for example, on intended corporate fusions. “Recommendations” and “Opinions” have no binding effect.

The “law of the European framework” includes the law of other European organizations. Particular attention should be made to the CoE with the ECHR. The ECHR is an

³³¹ CJEU. Judgment of the Court (Grand Chamber) of 8 March 2011, *Lesoochránárske zoskupenie VLK v Ministerstvo životného prostredia Slovenskej republiky*, Case C-240/09, ECLI:EU:C:2011:125. Para. 30.

³³² CJEU. Judgment of the Court of 30 April 1974, *R. & V. Haegeman v Belgian State*, Case 181-73, ECLI:EU:C:1974:41. Paras. 4–6

international agreement. Its rules therefore justify and oblige only its Member States but do not in themselves produce direct legal effect within national law; this requires a national implementation. The ECHR thus differs from European law in the strict sense, whose rules, according to the principle of the application of Union law, can apply directly without the need of a national implementing act.

2. Primary law regarding data protection

Until the entry into force of the Treaty of Lisbon, Art. 286 of the “Treaty establishing the European Community” (EC Treaty)³³³ was the only legislative basis for the regulation of data protection law. Today, there are mainly three provisions in primary law, with partly overlapping regulatory focus: Art. 16 TFEU, Art. 39 TEU, and Arts. 7 and 8 of the Charter.

2.1. Art. 16 TFEU

Art 16(1) TFEU recognizes the right to data protection, by stating that “everyone has the right to the protection of personal data concerning them”. Art. 16(1) TFEU goes far beyond the content of the former Article 286 of the EC Treaty and establishes the fundamental right of data protection which is also guaranteed in Art. 8(1) of the Charter. This additional anchoring means that the claim of an individual based on Art. 16(1) TFEU applies in addition to that of Arts. 7 and 8 of the Charter.

Art. 16(2), the TFEU provides for a uniform legislative power of the EU for the adoption of secondary law in the field of data protection law; Art. 16(2) TFEU sets forth that

the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Art. 16(2) TFEU thus resolves the principle of interdependence between the internal market and data protection. Formerly dependent on the legal basis in Art. 286 of the EC Treaty, the Union can now establish an independent right of data protection for all policy areas, regardless of whether this is necessary for the functioning of the internal market (Art. 114 TFEU). A special provision exists with Art. 39 TEU only for data processing in the area of the Common Foreign and Security Policy. The result is that Art. 16(2) TFEU is of comprehensive nature and a procedure of EU legislature can start whenever “activities” of the national stakeholders fall within the scope of the Union law, an easy presumption to fulfill in data protection subject matters, taking into account that data protection is a cross-sectional area.

The competence of the Union to regulate free movement of data is a *lex specialis* of general internal competence (Art. 114 TFEU), which was the legal basis for the Union’s existing legal acts addressed to the Member States. On this specific basis, the Union has set up sector-specific Directives on the processing of personal data.

³³³ European Communities. *Treaty establishing the European Community (Consolidated version 2002)*, OJ C 325, 33–184, (24 December 2002). (“EC Treaty”).

2.2. Art. 39 TEU

The Treaty of Lisbon integrated the second and third pillar of the EU into the EU treaties. Art. 39 TEU³³⁴ does not include a right to the protection of personal data, but a special procedure for exercising the EU's competence to regulate data processing in the area of Foreign and Security Policy. However, this does not mean that the right to the protection of personal data in these areas has not been granted. The right to the protection of personal data under Art. 16(1) TFEU, Arts. 7 and 8 of the Charter, as well as Art. 8 ECHR also applies to the actions of the EU and the Member States in the field of the Common Foreign and Security Policy.

2.3. Arts. 7 and 8 of the Charter

The Community treaties were classified as traditional international agreements, and thus a written list of fundamental rights was initially not considered necessary. However, as it became clear that the Community treaties were addressed not only to the Member States, but also to private individuals, several national constitutional courts found that Community action had to be measured against national fundamental rights. Accordingly, national courts claimed to declare secondary Community law in the country as inapplicable if, and in so far as, it conflicts with national fundamental rights.³³⁵ The CJEU had opposed this assessment and insisted on the primacy of Community law.³³⁶ However, it acknowledged that the solution could be to guarantee a comprehensive and effective protection of fundamental rights at Community level.

Based on its competence to protect the law (now Art. 19(1) TEU), the CJEU developed fundamental guarantees in the form of general principles of law. This development of the protection of fundamental rights begins with the CJEU's 1969 judgment in *Stauder*³³⁷: Following the interpretation of a fundamental right in national law, the CJEU established the foundation for the protection of fundamental rights in Community law. For the dogmatic reasoning of this jurisprudence, the explanations of the Attorney-General Mr. *Römer* are of importance. He argued that through a comparison of values to be found in essential values of national constitutional law, in particular the national fundamental rights, these can be seen as an unwritten element of Community law.³³⁸ The CJEU does not rely solely on national fundamental rights of a Member State and does not itself apply national fundamental rights, but rather sees in them a source of legal recognition for the determination of the unwritten fundamental rights of the Union. The CJEU later specified

³³⁴ "In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

³³⁵ Italian Constitutional Court. Sent. 183/7. // German Constitutional Court. BVerfGE 37, 271 ff. ("Solange I").

³³⁶ CJEU. Judgment of the Court of 15 July 1964, *Flaminio Costa v E.N.E.L.*, Case 6-64. ECLI:EU:C:1964:66, European Court reports 1964, 1251 ff. P. 1270.

³³⁷ CJEU. Judgment of the Court of 12 November 1969, *Erich Stauder v City of Ulm – Sozialamt*, Case 29-69, ECLI:EU:C:1969:57, European Court reports 1969, 419–426. P. 419.

³³⁸ CJEU. Judgment of the Court of 15 July 1964. *Flaminio Costa v E.N.E.L.*, Case 6-64. ECLI:EU:C:1964:66, European Court reports 1964, 1251 ff. P. 1270.

³³⁸ CJEU. Judgment of the Court of 12 November 1969, *Erich Stauder v City of Ulm – Sozialamt*, Case 29-69, ECLI:EU:C:1969:57, European Court reports 1969, 419–426. P. 427 ff.

its position in the cases *Internationale Handelsgesellschaft*³³⁹ and *Nold*³⁴⁰ that human rights are an integral part of the general principles of Community law and that as such the CJEU was bound to draw inspiration from the constitutional traditions common to the Member States. Therefore, the CJEU cannot uphold measures which are incompatible with fundamental rights recognized in the constitutions of Member States. The CJEU also found that “international treaties for the protection of human rights on which the Member States have collaborated or of which they are signatories, can supply guidelines which should be followed within the framework of Community law”³⁴¹. Until the recognition of the fundamental rights of the EU became a written component of primary law, fundamental rights of the Union – except several punctual written guarantees, e.g., today’s Art. 18 TFEU and Art. 157 TFEU – were derived from case law of the CJEU. Nor did the Treaties of Maastricht and Amsterdam³⁴² alter this, since, although they did contain standardization of fundamental rights, their mere character of a source of legal recognition remained.

The fact that there was no written catalog of fundamental rights and that the concretization of such unwritten rights was left over to CJEU jurisprudence always met criticism. Against the backdrop of this history, the need to enshrine EU fundamental rights in a binding text became increasingly apparent. The Council therefore commissioned a Convention in 1999³⁴³ to draw up an appropriate catalog and stated that “there appears to be a need, at the present stage of the Union’s development, to establish a Charter of fundamental rights in order to make their overriding importance and relevance more visible to the Union’s citizens”.³⁴⁴ The Convention submitted the Charter on 2 October 2000. In addition, the Presidency of the Convention drew up the “Explanations”³⁴⁵ on the individual provisions of the Charter, presented on 11 October 2000, which are of not inconsiderable weight for the interpretation of the Charter. The Charter was solemnly proclaimed on 7 December 2000 by the European Parliament, the Council and the Commission.³⁴⁶

The Convention elaborated the draft Charter with a view to possible incorporation into the Treaties. The European Parliament also advocated its inclusion in the EU’s legal texts. However, the decision of whether the document should be binding was postponed. It was not until 1 December 2009 when the Charter became legally binding with the entry

³³⁹ CJEU. Judgment of the Court of 17 December 1970, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, Case 11-70, ECLI:EU:C:1970:114. P. 1134. The court held that “However, an examination should be made as to whether or not any analogous guarantee inherent in Community law has been disregarded. In fact, respect for fundamental rights forms an integral part of the general principles of law protected by the court of justice. [...] The protection of such rights, whilst inspired by the constitutional traditions common to the Member States, must be ensured within the framework of the structure and objectives of the Community. It must therefore be ascertained, in the light of the doubts expressed by the *Verwaltungsgericht*, whether the system of deposits has infringed rights of a fundamental nature, respect for which must be ensured in the Community.”

³⁴⁰ CJEU. Judgment of the Court of 14 May 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*, Case 4-73, ECLI:EU:C:1974:51. P. 507. The court held that “fundamental rights form an integral part of the general principles of law, the observance of which it ensures. In safeguarding these rights, the court is bound to draw inspiration from constitutional traditions common to the member states, and it cannot therefore uphold measures which are incompatible with fundamental rights recognized and protected by the constitutions of those states. Similarly, international treaties for the protection of human rights on which the member states have collaborated or of which they are signatories, can supply guidelines which should be followed within the framework of Community law.”

³⁴¹ CJEU. Judgment of the Court of 14 May 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*, Case 4-73. ECLI:EU:C:1974:51. P. 507.

³⁴² European Communities. *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts*, OJ C 340, 1–144, (10 November 1997). (“Treaty of Amsterdam”).

³⁴³ European Parliament. (4 June 1999). *Cologne European Council, Conclusions of the Presidency*. https://www.europarl.europa.eu/summits/kol2_en.htm.

³⁴⁴ European Parliament. (2023). *Introduction to the EU Charter of fundamental rights*. https://www.europarl.europa.eu/charter/press/index_en.htm.

³⁴⁵ EU. *Introduction to the EU Charter of fundamental rights*, Official Journal of the European Union, C 303/17, (14 December 2007).

³⁴⁶ European Parliament. (7 December 2000). *European Council – Nice, Conclusions of the Presidency, 7 - 10 June 2000*. https://www.europarl.europa.eu/summits/nice1_en.htm.

into force of the Treaty of Lisbon. However, contrary to the previous intention, the Charter was not made a part of the Treaties, but it was declared binding by the provision of Art.6(1) TEU. Thus, the Charter remained an independent document, which strengthened the special position of fundamental rights. The protection previously substantiated in secondary law by means of the Directive 95/46 thus raised to the level of primary law by the Charter.

While Art. 7 of the Charter addresses the right to respect for private and family life, home and communication, Art. 8 of the Charter regulates the fundamental right to privacy, in a narrow sense, the protection of personal data. The rights under Art. 7 of the Charter are equivalent to the rights guaranteed by Article 8 ECHR and have therefore the same scope, Art. 52 (3) of the Charter. This makes demarcation difficult at times.

The CJEU ruled in *Schrems II* in this respect

when the fundamental right to respect for private life enshrined in Art. 7 of the Charter is affected by means of processing an individual's personal data, the right to data protection is also affected, as such processing falls within the scope of Art. 8 of the Charter, and, accordingly, must necessarily satisfy the data protection requirement laid down in that article.³⁴⁷

The CJEU already applied both fundamental rights in parallel before:

Respect for private life with regard to the processing of personal data, recognized by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 52).³⁴⁸

In the case of personal data not related to private life, on the other hand, only Art. 8 applies, Art. 8 of the Charter is then *lex specialis* to Art. 7 of the Charter.

These fundamental rights convey a defense right against interferences. They are enforceable rights and commit the Union and its institutions. The Member States are obliged to the extent that they are implementing Union law (Art. 51(1) of the Charter). We agree with Naef who found that Art. 8 of the Charter “has an extraterritorial dimension that applies to cross-border flows of personal data. The extraterritorial dimension of Article 8 CFR affords individuals in the EU continuous protection of personal data – essentially equivalent to that guaranteed within the EU – in the case that personal data is transferred from the EU to a third country”³⁴⁹. Interpretations of the CJEU in *Schrems I / II*, which were also based on Art. 8 of the Charter, also make Naef's opinion seem correct that “continuous protection of personal data is an unwritten constituent part – in addition to the six written constituent parts – enshrined in Article 8 CFR”³⁵⁰, therefore also concerns scenarios of TFPD to third countries, and “the export of personal data from the EU must be restricted to accord with this unwritten constituent part of Article 8 CFR”³⁵¹.

It is important to highlight the scope of protection regarding mail, postal and telecommunications secrecy, as well as modern forms of communication such as e-Mail.

³⁴⁷ *Schrems II*. Paras. 170–171

³⁴⁸ CJEU. Judgment of the Court (First Chamber) of 3 October 2019, *Staatssecretaris van Justitie en Veiligheid v A and Others*, Case C 70/18, ECLI:EU:C:2019:823. Para. 54

³⁴⁹ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 423.

³⁵⁰ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 423.

³⁵¹ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 424.

This distinction is relevant regarding the scope of application of the “E-Privacy Directive”³⁵², which comes into question when qualifying electronic communications services. As the CJEU noted, the obligation imposed on these providers “to retain traffic data for the purpose of making it available, if necessary, to the competent national authorities, raises issues relating to compatibility with Articles 7 and 8 of the Charter”.³⁵³ The same applies to other types of data processing, such as the transmission of data to persons other than users or access to that data with a view to its use, which, thus, entails an interference with those fundamental rights. Moreover, access to the data by a public authority constitutes a further interference, according to settled case-law.³⁵⁴

As with any other fundamental right recognized by the Charter, the exercise of the rights to privacy and data protection enshrined respectively in Arts. 7 and 8 may only be limited under the circumstances provided for in Art. 52(1) of the Charter. Hence, any such limitation must be (i) provided for by law and (ii) respect the essence of those rights and freedoms.³⁵⁵ Moreover, “[s]ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.”³⁵⁶

Therefore, limitations of the exercises of these rights may not be particularistic or ad hoc. As all other fundamental rights in the Charter, those recognized in Arts. 7 and 8 are not absolute rights but must be considered in relation to their function in society. The Charter therefore includes in Art. 52(1) – similar to Art. 29(2) of the “Universal Declaration of Human Rights” (UDHR)³⁵⁷ – a necessity and proportionality test to frame those limitations. The application of this test usually considers three steps: (i) is the measure suitable to achieve a legitimate aim?; (ii) is the measure “strictly necessary”³⁵⁸ to achieve that aim or are less restrictive measures available?; (iii) does the measure impose an excessive burden on the data subject? Thus, the limitation has to be “properly balanced” against the right at issue.³⁵⁹ In this respect, Naef found correctly that

no lawful limitations are possible in cases in which systematic, structural, and continuous data transfers take place to a third country that does not provide a level of protection for personal data that is essentially equivalent to that guaranteed within the EU. The interference with Article 8 CFR [Charter] caused by systematic, structural, and continuous data transfers fails the proportionality assessment in Article 52(1) CFR [Charter].³⁶⁰

The CJEU also argued in this way in the *Schrems* judgments, thus influencing the application of Chapter V of the GDPR.³⁶¹ The CJEU held that and unjustifiable interference with the rights to privacy and data protection enshrined in Arts. 7 and 8 of

³⁵² European Communities. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, Official Journal L 201, 37–47, (31 July 2002). (“E-Privacy Directive”). // *Nota bene*: In some sources also called the “Cookie Directive”.

³⁵³ CJEU. Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Other*, Case C-623/17, ECLI:EU:C:2020:790. Para. 60.

³⁵⁴ EDPB. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, (10 November 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf. P. 7.

³⁵⁵ Art. 52(1) of the Charter

³⁵⁶ Art. 52(1) of the Charter

³⁵⁷ UN. *Universal Declaration of Human Rights*, <https://www.un.org/sites/un2.un.org/files/udhr.pdf>, (10 December 1948).

³⁵⁸ CJEU. Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Other*, Case C-623/17, ECLI:EU:C:2020:790. Para. 68.

³⁵⁹ CJEU. Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Other*, Case C-623/17, ECLI:EU:C:2020:790. Para. 68.

³⁶⁰ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 424.

³⁶¹ See below Chapter II, Section II.3.4.4.

the Charter may be found regardless of “whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.”³⁶². According to the CJEU, legislation leading to an interference with these rights in the Charter “must lay down clear and precise rules governing the scope and application of the measure and imposing minimum safeguards, so that data subjects have sufficient guarantees that personal data will be effectively protected against the risk of abuse”, in particular where personal data are subjected to automatic processing and “where there is a significant risk of unlawful access to that data.”³⁶³ The four European “Essential Guarantees” intend to further specify how to assess the level of interference with the fundamental rights to privacy and to data protection.³⁶⁴

2.4. Internal and external perspectives: Arts. 51, 52, 53 of the Charter in relation with Art. 6 TEU

The Charter strengthens the relationship between rules of Union law and that of the ECHR. While Arts. 51 and 52 of the Charter concern the relationship between the fundamental rights in the European area and thus the “internal perspective” of this interpretation, Art. 53 seeks to safeguard the protection level also in the outer European dimension and thus the “external perspective”.

Art. 6(1) TEU stipulates that the Charter, TEU and TFEU are of equal legal rank. Therefore, the fundamental rights of the Union do not go beyond the rest of the Treaties nor fall behind it. This also applies to the general principles of Union law, which play an important role in the relationship with the ECHR, because fundamental rights which are guaranteed in the ECHR and which are a result from unwritten constitutional traditions of the Member States form part of primary union law, Art. 6(3) TEU. These general principles have a twofold character: on the one hand, they are to be considered when interpreting rights in the Charter (see Arts. 52(3) and (4) of the Charter); on the other hand, they continue to be used - as they entered into force before the Charter – for the development of fundamental rights. As soon as written norms of the Charter overlap with the unwritten general principles, the Charter applies.

In addition, Art. 6(2) TEU provides for the EU to accede to the ECHR. Protocol No. 14 to the ECHR of 13 May 2004 opened this option for EU accession since Art. 59(2) ECHR has been amended accordingly.³⁶⁵ Access to the ECHR would be fulfilled through an agreement between the contracting States of the ECHR and the EU. The negotiations on the EU’s accession culminated in a draft contract on 5 April 2013, which was submitted to the CJEU for examination.³⁶⁶ But, on 18 December 2014, the CJEU, which had been asked to provide an opinion under Article 218(11) TFEU, concluded that the accession agreement is not compatible with EU law. Its opinion condemned the draft agreement outright.³⁶⁷ The court found that the draft agreement was incompatible with Article 6(2) TEU and with Protocol No. 8 regarding Article 6(2) TEU. After the opinion of the CJEU, the accession of the EU to the ECHR remains an unfinished debate. On 7

³⁶² Schrems II, Para. 171

³⁶³ CJEU. Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Other*, Case C-623/17, ECLI:EU:C:2020:790. Para. 68.

³⁶⁴ See below Chapter IX, Section III.3.

³⁶⁵ CoE. *Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention*, Treaty No.194, (13 May 2004).

³⁶⁶ CoE. (5 April 2013). *Fifth Negotiation Meeting between the CD DH ad hoc Negotiation Group and the European Commission on the accession of the European Union to the European Convention on Human Rights*. http://www.echr.coe.int/Documents/UE_Report_CDDH_ENG.pdf.

³⁶⁷ CJEU. *Opinion of the Court (Full Court) of 18 December 2014*. Case Opinion 2/13. ECLI:EU:C:2014:2454.

October 2019, after it received a written contribution from the Commission which addressed all the objections raised by the CJEU, the Council reaffirmed its commitment to the accession and agreed on supplementary negotiating directives to allow for a swift resumption of negotiations with the CoE.³⁶⁸ On 29 September 2020, the negotiations between the Commission and the Member States of the CoE on the accession of the EU to the ECHR were resumed. In the event of accession, the question of the relationship and delimitation of competences between the CJEU and the ECtHR would arise. In this context, the CJEU could not evade fundamental rights control by the ECtHR, as the credibility of the Union in the field of human rights would be at stake. Therefore, Protocol No. 8 regarding Article 6(2) TEU established constitutive elements of the legal order of the EU that must be respected in an accession agreement.

Art. 52(3) of the Charter does not explicitly preclude a broader scope of protection than that granted in the ECHR. Likewise, the constitutional traditions of the Member States may go beyond the scope of the ECHR. Thus, the standard of the ECHR is only a minimum limit. The ECHR, however, influences the fundamental rights of the Union as a source of legal recognition in two aspects. On the one hand, the rights in the Charter which correspond to the rights guaranteed by the ECHR have the same meaning and scope. On the other hand, the Union has to orient itself to the ECHR as a General principle of union law under Art. 6(3) TEU. If fundamental rights – which are also standardized in the ECHR – are concerned, and if the ECtHR has issued a jurisprudence in respect to these rights, it is also up to the national courts to take account of the ECtHR findings. The references of Charter and TEU to the ECHR are not static, but dynamic. This means that future changes in the ECHR are also to be considered. Art. 52(3) of the Charter is thus a “transfer” or “homogeneity” standard, which is intended to ensure the compatibility between the Charter and the ECHR.

International organizations and countries which are not EU members are not bound by the fundamental rights of the Union (Art. 51(1) of the Charter). If the EU concludes international agreements, these are acts of the Union, which must be measured against the fundamental rights of the Union. The agreements concluded by the Union shall bind them and the Member States firstly under international law, and secondly in accordance with Union law (Art. 216 TFEU). The binding nature of Union law is precedent to secondary law; but insofar as international law itself protects human rights, this must be taken into account when interpreting the Charter in accordance with Art. 53 of the Charter.

3. Secondary law regarding data protection

Legislation on data protection at Member State level by means of secondary law had been based on Art. 95 of the EC Treaty (now Article 114 TFEU) until the entry into force of the Treaty of Lisbon. The Parliament was equally involved in the legislative process and the secondary legislative elements were created by the Parliament and the Council, as proposed by the Commission. Later, non-constitutional competencies were added both in the second pillar of the “Common Foreign and Security Policy” (CFSP) and in the third pillar of “Police and Judicial Co-operation in Criminal Matters” (PJCCM) because problems appeared in these pillars being the lack of involvement of the Parliament which led to a lack of competence in the adoption of data protection regulations. This escalated

³⁶⁸ Council of the European Union. (7 October 2019). *10th anniversary of the Charter of fundamental rights: Council reaffirms the importance of EU common values*. <https://www.consilium.europa.eu/en/press/press-releases/2019/10/07/10th-anniversary-of-the-charter-of-fundamental-rights-council-reaffirms-the-importance-of-eu-common-values>.

in the cases regarding PNR³⁶⁹ and data retention³⁷⁰. Problems related to inner-EU competencies, such as transfer of PNR and data retention significantly reduced with the entry into force of the Treaty of Lisbon.

All secondary legislation of the Union is compatible and complementary to laws of the CoE. This means that secondary legislation adopts the principles set out in these laws and supplements them. Arts. 7 and 8 of the Charter are based on Art. 52(3) of the Charter. Recital 10 of Directive 95/46 points out that “the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community”. Recital 11 adds: “Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive [95/46], give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data”. This ensures that in principle no divergences occur in the cumulative consideration of these two legal sources for the interpretation of Art. 16 TFEU. With regard to Art. 8 ECHR, the CJEU has already decided that Directive 95/46 should not be interpreted as being able to justify an impairment of the right to respect for private life contrary to Art. 8 ECHR. The principle of compatibility of secondary union law with the laws of the CoE must also apply to future data protection provisions of EU law. They are also to be measured against this standard and must not be left behind it. In addition, this is not only about the defense of data protection law, and thus the self-determination of the individual, but also about ensuring transborder data transfer, which shows a double direction.

3.1. Directive 95/46

The first instrument of secondary law adopted by the EU was Directive 95/46. This Directive was eventually repealed by the current GDPR, adopted in 2016. However, Directive 95/46 had an essential importance for the development of the European data protection framework, particularly through the CJEU interpretations of the provisions of Directive 95/46 which have an equivalent provision in the GDPR, as that guidance must still to be taken into account when applying the GDPR. Therefore, we provide explanations of the Directive 95/46 in this thesis.

In January 1981, Convention 108 was opened for signature. By 1985, when Convention 108 had been ratified by five countries, the harmonization of data protection law in the EC began at supranational level. However, the Commission, which had the initiative monopoly for the legislation of the EC (and now also for the EU), decided to make a proposal only in 1990.³⁷¹ The main driver of Directive 95/46 was the harmonization of substantive data protection law. It is almost forgotten nowadays that the primary objective of the Commission was to allow a free flow of data.³⁷² The European Parliament also made a strong contribution to the second target: the protection of personality.

Looking at the rules on material- and personal scope, it is noticeable that the Community’s legislature focused on the widest possible scope of application. According to Art. 3(1) Directive 95/46, the partial automated processing of personal data was also

³⁶⁹ CJEU. Judgment of the Court (Grand Chamber) of 30 May 2006, *European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04)*, Cases C-317/04 and C-318/04, ECLI:EU:C:2006:346.

³⁷⁰ CJEU. Judgment of the Court (Grand Chamber) of 10 February 2009, *Ireland v European Parliament and Council of the European Union*, Case C-301/06, ECLI:EU:C:2009:68.

³⁷¹ Commission of the European Communities. *Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data*, Procedure 1990/0287/COD, COM (1990) 314 - 2, (18 July 1990).

³⁷² European Commission, COM/90/314FINAL, 13 September 1990. Para. 15, which states “in order to remove the obstacles to the exchange of data which is necessary if the internal market is to function”

included when a file is stored. According to Art. 2(a) Directive 95/46, the identifiability of the person is sufficient for the information to be considered personal data; the processing of data is subject to all data types of handling (Art. 2(b) Directive 95/46); and the definition of data access (Art. 2(c) Directive 95/46) is also far-reaching. More important for the transborder aspect was the country-of-origin principle in Art. 4(1)(a) Directive 95/46. According to this principle, the applicable law is that of the State in which the responsible body – i.e., the person who determines the purposes and means of the processing – is based. The wording of Art. 4(1)(a) Directive 95/46 establishing this principle gave rise to various legal opinions which led to interpretations by the CJEU in several cases.

The “*Google Spain*” case³⁷³ was concerned with jurisdictional questions affecting TFPD. In this judgment, the CJEU affirmed the applicability of European data protection law to providers which have a European branch promoting the sale of advertising space. The decisive factor in this respect was not the payment of a fee for the use of a service, but that there is an offer aimed at customers residing in a Member State of the Union. The claim to also cover transborder facts is thus linked to a data processing that is related to the activities of an establishment in the EU territory – and is therefore ultimately based on the principle of territoriality. However, the CJEU did not claim extraterritorial jurisdiction to enforce for the Union, but merely enforced the conditions of access to the EU’s internal market. This was a broad interpretation of the scope of application of Directive 95/46, which, however, was necessary to ensure its effectiveness and a comprehensive protection of fundamental rights.

This interpretation by the CJEU made it more difficult for companies to circumvent the European level of protection through a choice of the head office of the parent company (so-called “forum shopping”). Forum shopping is understood as the systematic exploitation of jurisdictions that may exist side by side in several countries, to obtain certain legal advantages, as – in view of the legal practice of courts – it can make sense for the plaintiff to choose a specific place of jurisdiction in the world. In individual cases, forum shopping is generally permitted, however, there may be a legal abuse of the place of jurisdiction, for example if a court is obviously not chosen on the basis of preferences that appear to be advantageous, but solely because it is geographically as far away as possible from the opponent.³⁷⁴ Forum shopping could endanger the determination of applicable law and jurisdiction regarding TFPD whenever interferences with data subject rights are conducted in a virtual environment. For forum shopping in the international area, the following conditions must be checked and weighed against each other: Duration of the respective procedures, costs, tendencies of jurisprudence, efficiency of interim legal protection, advantages and disadvantages of the respective civil procedure code. In *Weltimmo* – a CJEU judgment of 1 October 2015, overshadowed by the CJEU’s judgment in the *Schrems I* case – the key question was the correct meaning of the term “establishment”.³⁷⁵ The CJEU stressed the need for a flexible definition of the term, rather

³⁷³ Google Spain case.

³⁷⁴ *Kammergericht, Fliegender Gerichtsstand*, 5 W 371/07, 25 January 2008. P. 212.

³⁷⁵ CJEU. Judgment of the Court (Grand Chamber) of 1 October 2015, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, ECLI:EU:C:2015:639. (“*Weltimmo* case”). Para. 41. In this judgment, the CJEU ruled that “in the light of all the foregoing considerations, the answer to the first to sixth questions is as follows: – Article 4(1)(a) of Directive 95/46 must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity – even a minimal one – in the context of which that processing is carried out; – in order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State’s language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the

than a formalistic approach whereby undertakings are established solely in the place where they are registered. Therefore, an establishment is sufficient in the territory of the Member State in question where the company shows effective activity in which the processing is carried out, even if the activity is only marginal. If the CJEU would have ruled in the *Google Spain* case that Google Inc. and *Google Spain* were separate for the purpose of Art. 4(1) Directive 95/46, then the relevant processing would have been beyond the reach of Directive 95/46. As a result, there might have been no “effective and complete protection of the fundamental rights and freedoms of natural persons”, data subjects might have been “deprived of the protection guaranteed by the directive” and the company responsible could have been seen to “escape the obligations and guarantees laid down by Directive 95/46”.³⁷⁶ In contrast, in *Wirtschaftsakademie Schleswig-Holstein* (also known as the “Facebook fanpages case”), under a finding that Facebook Inc and Facebook Germany are separate for the purpose of Article 4(1)(a), Union law would still apply.³⁷⁷

The dispute between the Austrian consumer protection association (*Verein für Konsumenteninformation*) and Amazon EU Sàrl (Amazon EU) also included the interpretation of Art. 4(1)(a) Directive 95/46.³⁷⁸ The dispute arose from Amazon EU’s use of a choice of laws clause nominating Luxembourg law also for Austrian consumers – an approach which the Austrian consumer protection association considered to be contravening EU law. The CJEU ruled that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if the undertaking carries out the data processing in question in the context of activities of an establishment situated in that Member State. It is for the national court to ascertain whether that is the case.³⁷⁹

Under Directive 95/46, two requirements were to be met for transferring personal data from an EU Member State to a “third country” (country outside the territory of the EU and the European Economic Area). Firstly, the processing had to comply with the applicable national requirements to lawfully process personal data in that Member State or EEA Member Country (“first stage test”). Secondly, the level of data protection in the third country must be assessed to ensure that the third country in question offers an adequate level of protection (“second stage test”).

To comply with the latter, Art. 25(1) Directive 95/46 provided that the transfer of personal data which “are undergoing processing or are intended for processing after the transfer” may only take place if the “third country in question ensures an adequate level of protection”. Adequacy shall be assessed in the light of all circumstances surrounding the data transfer in question, in particular the nature of personal data, the purpose and duration of processing, country of origin and country of final destination, the rule of law and professional rules and security measures (Art. 25(2) Directive 95/46). Whenever the Commission found that a third country does not ensure an adequate level of protection, Member States had to take the necessary measures to prevent the transfer (Art. 25(4) Directive 95/46).

controller in the administrative and judicial proceedings relating to the processing of the data concerned; – by contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.”

³⁷⁶ *Google Spain* case. Paras. 53–58.

³⁷⁷ CJEU. Judgment of the Court (Grand Chamber) of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd*, C 210/16, ECLI:EU:C:2018:388. (“Facebook fanpages case”).

³⁷⁸ CJEU. Judgment of the Court of 28 July 2016, *Verein für Konsumenteninformation v Amazon EU Sàrl*, C-191/15, ECLI:EU:C:2016:612. (“*Verein für Konsumenteninformation* case”).

³⁷⁹ *Verein für Konsumenteninformation*. Para. 82

Art. 25(6) Directive 95/46 entitled the Commission to determine that a third State ensures (either as a whole or for specific areas) an appropriate level of protection regarding the protection of the freedoms and fundamental rights of individuals. Such a finding was made in several cases, including in the case of the Safe Harbor Privacy Principles issued by the US Department of Commerce. The Safe Harbor agreement as such was not the legal basis for the transfer of data to the US; rather, the basis was the adequacy decision made by the Commission according to Arts. 31(2) and 25(6) Directive 95/46. To prevent contrasting decisions in determining whether a third country has an appropriate level of protection, Directive 95/46 specified a certain procedure. In accordance with Arts. 29 and 30 Directive 95/46, the WP29 – after having received opinions from independent bodies – provided a report to the Commission. This procedure was also intended to ensure the participation of the governments of the Member States, thereby assisting the Commission in the exercise of its decision-making power (Art. 31(2) Directive 95/46). In accordance with Arts. 25(4) and (6) Directive 95/46, the procedure for assessing the adequacy of the level of protection in third countries referred to both positive and negative outcomes, which were binding for Member States.

In addition to the principle set out in Art. 25(4), Directive 95/46 addressed the aim of a free flow of data by providing in its Art. 26(1) a comprehensive list of derogations so that a transfer of personal data to a third country without an adequate level of protection may still be carried out. A Member State was able to authorize the transfer if the controller proved “additional safeguards”³⁸⁰ for the protection of the rights of the data subject, Art. 26(2) Directive 95/46. These derogations covered a variety of transfers of personal data to third countries. However, there were areas where none of those were applicable. Examples were MNEs centrally processing data from employees and customers. On the one hand, transnational organizations and the use of existing resources required an unhindered exchange of data, while on the other hand, in these cases, the gathering of data subjects’ consent was often not possible in practice.

Where adequate protection was not ensured and where none of the relevant derogations were applicable, the data transfer in question had to be blocked, which in practice threatened a free flow of data. The Commission had considered this when it was faced with the European-American disputes over adequacy, and commissioned a survey on data protection law and data protection practice in the US in the Annex to the Second Annual Report in 1998 of the WP29.³⁸¹ The assessment method of the data protection group for adequacy which was outlined in a WP29 synthesis paper was also tested in a study by the University of Edinburgh.³⁸² The disadvantage of this procedure was that few (14) countries had been recognized by the European Commission to meet the adequacy level, illustrating the slowness of the adequacy process.³⁸³ This process was complicated by political factors: an adequacy decision needed to be prepared by a study by the

³⁸⁰ At this point, reference must be made to *termini technici* that may be confusing for the reader. Under Directive 95/46, these are called “additional safeguards”, while the GDPR calls them “appropriate safeguards”. Further below (Chapter II, Section II.3.4.4.g.) we will see that “supplementary measures” may be necessary according to *Schrems II*; these measures are to be understood as such in addition to “appropriate safeguards” (GDPR).

³⁸¹ WP29. *Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten*, GD XVD/5047/98, WP 14, (30 November 1998).

³⁸² WP29. *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, GD XVD/5025/98, WP 12, (24 July 1998). // Raab C. [Charles] et al. (1999). *Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: Test of the method on several categories of transfer*. Office for Official Publications of the European Communities.

³⁸³ “The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection. With the exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of Directive (EU) 2016/680).” European Commission. (11 April 2023). *Adequacy decisions*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Commission on the legal system of the country in question. Such studies required highly specialized linguistic, legal and data protection expertise, with which the European Union seemed not be provided with at this point of time. The process of adequacy concerning the Argentine system was an example for political interference. Several data protection authorities had “misgivings as to whether the Argentine system should be found adequate, but the decision was ultimately approved because of politics”.³⁸⁴

To avoid impacts on US-EU data transfers by the annulment of Safe Harbor (*Schrems I*), authorities on both sides took benefit of the provision in Art. 25(5) Directive 95/46, which instructed the Commission to enter negotiations on the further orientation in this legal area. The Commission saw the necessity to give further assistance and issued on 6 November 2015 a guidance for companies setting out alternative bases allowing TFPD to the US.³⁸⁵

The Council and the Parliament had given the Commission the power to decide that SDPC as such alternative base can offer additional safeguards as required by Art. 26(2) Directive 95/46. The Commission had adopted three “Sets” of SDPC based on Art. 26(4) Directive 95/46:

- SDPC for the transfer of personal data to third countries³⁸⁶, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016³⁸⁷ (“Set I” or “2001 SDPC”);
- Alternative SDPC for the transfer of personal data to third countries (“Set II” or “2004 SDPC”)³⁸⁸;
- SDPC for the transfer of personal data to processors established in third countries³⁸⁹, which were amended in 2016 by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016³⁹⁰ (“Set III” or “2010 SDPC”).

Two Sets are related to data transfers between controllers, while the last applies to data transfers between controller and processor. Clauses already adopted under Directive 95/46 continue to apply under the GDPR (Art. 46(5) GDPR) and will thus be analyzed below more in detail.³⁹¹

³⁸⁴ Kuner, C. [Christopher]. (2009). Developing an Adequate Legal Framework for International Data Transfers. In S. [Serge] Gutwirth and Y. [Yves] Poullet and P. [Paul] de Hert and C. [Cécile] and S. [Sjaak] Nouwt (ed.), *Reinventing Data Protection?* (pp. 263–275), Springer. P. 265.

³⁸⁵ European Commission. *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14*, COM(2015) 566 final, (6 November 2015).

³⁸⁶ European Commission. (15 June 2001). *Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC*, 2001/497/EC, OJ L 181, 19–31.

³⁸⁷ European Commission. (16 December 2016). *Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council*, OJ L 344, C/2016/8471, 100–101.

³⁸⁸ European Commission. (29 December 2004). *Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries*, OJ L 385, 2004/915/EC, 74–84.

³⁸⁹ European Commission. (5 February 2010). *Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council*, OJ L 39, 2010/87, 5–18.

³⁹⁰ European Commission. (16 December 2016). *Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council*, OJ L 344, C/2016/8471, 100–101.

³⁹¹ Chapter II, Section II.3.4.4.g.

BCR are also an alternative base to meet the requirements of additional safeguards to enable a lawful TFPD. BCR require a binding agreement between the company group's legal entities, which is to be approved by all competent SAs. The scope of an approval by a SA is disputable. It could be argued that, according to applicable law, not only the BCR are to be approved by the competent SA, but also every TFPD to a third country, based on BCR.

In the case of TFPD by organizations whose areas of activity extend beyond the area covered by the Privacy Shield principles, the Privacy Shield concept naturally reached its limits. Since Privacy Shield provided a solution for data transfer from the EU/EEA to the US, the system did not provide comprehensive answers for MNEs. These were still dependent on the above-mentioned alternatives such as SDPC and BCR.

3.2. E-Commerce Directive

To provide some legal certainty to the emergence of new services based on the Internet, and particularly the role of SPs in the new millennium, the EU developed a digital agenda that resulted in several policy papers and legal instruments. One of these instruments is the "E-Commerce Directive"³⁹² adopted in 2000, which aims to ensure that the internal market functions properly by ensuring the free movement of information society services between the Member States.

The E-Commerce Directive is a horizontally applicable regulatory instrument for the provision of information society services. It established some minimum harmonization criteria, set "duties of care" and "notice and take down" obligations to remove illegal online content, but also liability exemptions for intermediaries.

The E-Commerce Directive does not explicitly have an extraterritorial scope. The core idea of the E-Commerce Directive is the country-of-origin principle, which generally forbids that EU Member States impose restrictions on the provision of information society services from another Member State, in several areas known as the "coordinated field" (Art. 3(2) ECD). Member States are free to regulate activities of information society services providers which are based outside the EU/EEA, as the country-of-origin principle only applies to providers based in the EU.

A key element of the E-Commerce Directive is the exemption from liability for third party content, which is granted to several types of intermediary activities, namely mere conduit, caching and hosting services, laid down in Arts. 12–15 ECD. Accordingly, platform operators are not liable for content uploaded to their website unless they become aware of the illegality and are not acting adequately to stop it. This liability privilege is what made the emergence of the major platforms possible in the first place. It is therefore no coincidence that platforms such as Google and Meta subsequently grew strongly.

It was found that the implementation of the E-Commerce Directive in the national laws of the Member States has been very different, and also that some gaps have arisen.

First, it remains unclear to what extent the new type of online services, such as social media companies that have appeared since the adoption of the E-commerce Directive, fall within the definition of 'information society services' providers that can benefit from the liability exemption. Second, the "safe harbor" conditions and "notice-and-take down"

³⁹² European Communities. *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, Official Journal L 178, 1–16, (17 July 2000). ("ECD").

obligations are unclear essentially because the underlying notions which are used to trigger the liability exemption, such as the distinction between “passive” role and “active” and the meaning of “illegal activities”, lack a proper definition. There are also considerable differences both with regard to the definition and the functioning of notice-and-take down throughout the EU. Third, it is becoming difficult to differentiate between prohibited “general” content monitoring and acceptable “specific” content monitoring, while automatic filtering mechanisms are increasingly used to detect illegal content.³⁹³

In 2018, shortly before the GDPR came into force, the CJEU assessed the assignment of liability for data protection in a multi-level system of ISPs, such as the relationship between Facebook and an operator of a Facebook fan page.³⁹⁴ This assessment is relevant insofar as data protection law extends into the field of information obligations of ISPs. In these constellations, the intermediary is (also) responsible under data protection law due to the intermediate storage of personal data, which constitutes a processing of personal data. These providers then have to comply with the information obligations in terms of national tele media rights (e.g., in Germany the Telemedia Act³⁹⁵) or E-Commerce as well as data protection. The E-Commerce Directive does not make specific provisions regarding the protection of personal data, but it does regulate aspects that may also have an impact on the right to informational self-determination and the personal rights of users. For example, the E-Commerce Directive provides for comprehensive information obligations on the part of providers, which also relate to data protection.

ECD and Directive 95/46 apply alongside each other and must be examined separately. According to Art. 1(5)(b) ECD, the E-Commerce Directive does not apply to data protection issues concerning information society services, which are covered by Directive 95/46 and the E-Privacy Directive. Both Directive 95/46 and the GDPR are therefore fully applicable to information society services and must be fully observed when implementing and applying the ECD. Accordingly, Art. 2(4) GDPR now specifies that the GDPR “shall be without prejudice to the application of Directive 2000/31/EC [E-Commerce Directive], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.”

This parallel application can lead to considerable contradictions because data protection law as well as civil and criminal law provisions can provide for similar legal consequences for an intermediary regarding the same third-party content. In particular, the application of data protection law to the provision of third-party content threatens to undermine the liability privileges of host providers under Art. 14 of the ECD. The E-Commerce Directive has remained unchanged to this day, although it dates to 2000. Therefore, the Commission has signaled that it will rise to the challenge of overlaps in regulation, and there are indications that it will propose a revision or replacement of the to shape the digital economy at EU level as well as setting the standards for the rest of the world, as it did with data protection.³⁹⁶ The European Commission therefore proposed a new legal framework: the Digital Services Package, consisting of the Digital Services Act and the Digital Markets Act.³⁹⁷

³⁹³ Madiaga, T. [Tambiama]. (2020). *Reform of the EU liability regime for online intermediaries, Background on the forthcoming digital services act*. European Parliamentary Research Service. P. I.

³⁹⁴ CJEU. Judgment of the Court (Grand Chamber) of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd*, C 210/16, ECLI:EU:C:2018:388. (“Facebook fanpages”).

³⁹⁵ Federal Republic of Germany. *Telemediengesetz of 26 February 2007 (BGBl. I p. 179, 251), as last amended 12 August 2021 (BGBl. I p. 3544)*. (26 February 2007).

³⁹⁶ European Parliament. *Digital: The EU must set the standards for regulating online platforms, say MEPs*. (20 October 2020). <https://www.europarl.europa.eu/news/en/press-room/20201016IPR89543/digital-eu-must-set-the-standards-for-regulating-online-platforms-say-meps>.

³⁹⁷ European Commission. (2023). *The Digital Services Act package*. <https://ec.europa.eu/digital-single-market/en/digital-services-act-package>.

3.3. E-Privacy Directive / E-Privacy Regulation

The E-Privacy Directive came into force on 31 July 2002. It supplemented Directive 95/46 (until the GDPR started to apply) whenever personal data are processed in the field of electronic communications.³⁹⁸ The E-Privacy Directive is intended to provide protection for the right to privacy and confidentiality, but also to enable the free flow of data within the EU.³⁹⁹ To this end, it harmonizes provisions adopted by the Member States for the protection of personal data and privacy.⁴⁰⁰ The E-Privacy Directive applies “to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community” (Art. 1(1)). Unlike Directive 95/46, which only protects personal data of natural persons, the E-Privacy Directive also protects the legitimate interests of legal persons as participants in electronic communications.

The E-Privacy Directive contains rules to ensure the right to privacy and confidentiality of users when information is exchanged via electronic communications services, for example via mobile and landline telephony or e-mail. It lays down rules according to which providers of electronic communication services must guarantee the secure processing of personal data and to notify users in the event of a breach of the protection of personal data. It generally prohibits unsolicited messages for the purposes of direct marketing without prior consent of the user.

In addition, it protects users from violations of their right to data protection by cookies and other instruments that penetrate their PC, mobile phone or other terminal. Cookies and similar technologies are currently indispensable for website operators to provide both “essential” functions of the website and to fulfill “additional” (own) purposes such as advertising. Global online retailers rely heavily on information that they and third-party providers collect and analyze from visitors to their online offerings with the aid of cookies or comparable technologies. When cookies are used, not necessarily, but also personal data can be processed in addition to technical information. Art. 5(3) of the E-Privacy Directive applies regardless of whether this information is personally identifiable. Compared to the E-Privacy Directive, the GDPR - which determines in Recital 30 that cookies are also personal data - at first glance gives website operators more leeway for the lawful use of non-essential cookies. While Art. 5(3) E-Privacy Directive requires consent, a non-consent-based approach is also conceivable under the GDPR. In particular for website operators who use non-essential cookies, the question therefore arises at the latest with the entry into force of the GDPR as to how the E-Privacy Directive and the GDPR relate to each other in the case of such electronic communications.

This does not only apply for website operators but also for providers of “over-the-top content” (OTT). Since the last revision of the E-Privacy Directive in 2009⁴⁰¹, important new technological services such as OTT were introduced to the digital economy. So far, it has been controversial whether the E-Privacy Directive also applies to OTT. OTT are content, services or applications that are made available to an end user via the public Internet. OTT do not stand for a certain type of service, but for a certain method of

³⁹⁸ Recital 10 of the E-Privacy Directive: “Directive 95/46/EC applies to non-public communications services”

³⁹⁹ Recitals 2 and 3 of the E-Privacy Directive

⁴⁰⁰ Recital 8 of the E-Privacy Directive

⁴⁰¹ EU. *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws*, Official Journal of the European Union, L 337, (18 December 2009).

providing them, namely making them available via the public Internet. In its Digital Single Market Strategy the Commission had already announced a review of the E-Privacy Directive for the period after the adoption of the GDPR, in particular to ensure a high level of protection for the persons concerned and a level playing field for all market participants.⁴⁰² Most of the provisions of the E-Privacy Directive apply, in the opinion of the Commission, only to operators of conventional electronic communications services; in contrast, providers of information society services which use the Internet to provide communication services are generally excluded from their scope which led to an inadequate protection of the confidentiality of communication and the scope of the E-Privacy Directive should therefore be extended.⁴⁰³

The European Commission therefore presented in January 2017 an evaluation of the E-Privacy Directive and a proposal for an “E-Privacy Regulation”.⁴⁰⁴ This proposal was the start of the legislative process that has dragged on to this day. The aim is to review and renew the data protection rules for services of the electronic communication sector. These rules are also intended to apply to responsables which use electronic communication services to conduct direct advertising to end users or which collect information that is stored in or related to users’ end devices; ISPs are also to be covered by these rules.

Both E-Privacy Directive and proposed E-Privacy Regulation contain rules concerning the processing of personal data, which leads to the question about their relationship to the GDPR. Art. 95 GDPR stipulates that the GDPR “shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC” (the E-Privacy Directive). This is supported by Recital 173 of the GDPR, which says that the GDPR applies “to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural person”. Art. 1(2) of the E-Privacy Directive stipulates that the regulations of the E-Privacy Directive “particularize and supplement” Directive 95/46. Thus, to the extent that a specific issue relating to the processing of personal data falls within the scope of the E-Privacy Directive, the provisions of the GDPR are subordinate to those of the E-Privacy Directive, the E-Privacy Directive is then *lex specialis* to the GDPR. In turn, the GDPR remains applicable to matters relating to the processing of personal data in the field of electronic communication for which the E-Privacy Directive does not contain any specific regulations. Therefore, when examining the applicability of national laws of a Member State, it must be assessed whether the E-Privacy Directive already covers the facts of the case in question. If such a provision exists, it must also be assessed whether it has already been implemented in the respective national law of the Member State. If there is no relevant provision in the E-Privacy Directive, the GDPR as *lex generalis*

⁴⁰² European Commission. *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, (6 May 2015). P. 13.

⁴⁰³ The Commission was of the opinion that so-called OTT services were not covered by the E-Privacy Directive. See European Commission. (19 December 2016). *E-Privacy: consultations show confidentiality of communications and the challenge of new technologies are key questions*. <https://wayback.archive-it.org/12090/20190630043525/https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-communications-and-challenge-new-technologies-are>.

⁴⁰⁴ European Commission. (10 January 2017). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication*. <https://digital-strategy.ec.europa.eu/en/library/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector> // European Commission. *Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM(2017) 10 final, (10 January 2017). (“E-Privacy Regulation”).

applies as far as its scope applies. Art. 1(3) of the proposed E-Privacy Regulation provides that “the provisions of this Regulation particularize and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 to 2.” This could indicate that the rules in Arts. 6, 7 and 8 of the proposed E-Privacy Regulation are *lex specialis* and there is no room for the application of Art. 6 GDPR. However, other obligations and rules are at least partially regulated in the proposed E-Privacy Regulation and can also be found in the GDPR (e.g. Arts. 22 of the proposed E-Privacy Regulation and Art. 82 GDPR). It is not clear whether the specialty in the proposed E-Privacy Regulation goes so far that the corresponding regulations in the GDPR are completely excluded or only partially.

The proposed E-Privacy Regulation applies to the processing of electronic communications content relating to the provision and use of electronic communications services, Art. 2(1) of the proposed E-Privacy Regulation. Both content and metadata are included, Art. 4(2)(b). Same as the GDPR, the proposed E-Privacy Regulation will have a broad scope (Art. 3). The territorial scope also covers the protection of information related to the end user equipment of users in the EU (Art. 3(1)(a)). Thus, the proposed E-Privacy Regulation applies also to services outside the Union which are directed to end users in the Union (like the interpretation of Directive 95/46 in the *Google Spain* case). IoT is explicitly mentioned in Recital 14. However, the focus of the Commission lies not only on communication between device and end user, but also on the communication between two devices. Information that is exchanged between two devices within the networked industry and networked household appliances may also contain personal data within the meaning of the GDPR. Art. 8(1) of the proposed E-Privacy Regulation prohibits the use of the computing and storage capacity of a device and to collection of information from the end user’s equipment. There are a few exceptions to this principle. *Inter alia* if it is necessary for the sole purpose of transmitting the communication over an electronic communications network or if the end user has previously given consent to this data processing. No consent is required if the processing is necessary for providing an information society service requested by the end user. According to Art. 8(2) of the proposed E-Privacy Regulation, the gathering of data sent by a device to connect to another device or network is in principle also excluded; collection is permitted only if this serves exclusively the purpose of establishing a connection between the devices. Should such data be used for advertising purposes or profiling, the user has a right of objection as stipulated in Art. 21 GDPR. In addition, appropriate technical and organizational measures must be taken to create an appropriate level of safety, the proposed E-Privacy Regulation refers hereby to Art. 32 GDPR. Recital 28 of the proposed E-Privacy Regulation provides that software providers should be required to distribute software only with privacy-friendly settings. In addition, the Commission would like to allow users to choose their privacy settings when activating the software for the first time. If a user does not make any settings, the web browser should fall back to the presetting meaning that any storage by cookies of third Parties or other kind of purposes is not allowed. Art. 10 deals with the principle of Privacy by Design. According to paragraph 1, the settings of all components of a device which is distributed in the European market must provide per default that third Parties can neither store information nor collect information from this device. The proposed E-Privacy Regulation would also provide for certain regulations for the use of electronic communications services for advertising purposes. According to Art. 16(1) of the proposed E-Privacy Regulation, the use of electronic communications services for the purpose of the transfer of direct advertising is to be permitted only with the prior consent of the end user. Art. 16(2) of the proposed E-Privacy Regulation makes an exception whenever there is a customer relationship between the advertisers and the end user. Art. 11 of the proposed E-Privacy Regulation allows Member States to limit, under certain conditions, the rights and obligations laid down in Articles 5 to 8 of the proposed E-

Privacy Regulation. This possibility of limitation recalls those of the GDPR. The problem may arise that divergent rules can be introduced in the different Member States and the harmonization effect of the regulation is achieved only to a certain extent. Art. 19 of the proposed E-Privacy Regulation provides that the provisions of Chapter 2 of the proposed E-Privacy Regulation are to be monitored by the national SAs. Art. 19(2) of the proposed E-Privacy Regulation provides that these SAs are also responsible for monitoring compliance with the GDPR. Art. 25 of the proposed E-Privacy Regulation describes the requirements for the imposition of fines. These are largely based on the regulations of the GDPR (4% of the annual turnover of a company in the past financial year).

It is to be expected that the material scope of the proposed E-Privacy Regulation expands compared to the E-Privacy Directive and not only brings new requirements for data processing according to Art. 28 GDPR, but also to joint responsibility. This is because the draft of the proposed E-Privacy Regulation that exist to date contains requirements for the processing of electronic communication data, which the controller must then meet in the future. After the last draft was finally rejected on 22 November 2019, a new discussion paper was published on 6 July 2020 as part of the German Council Presidency.⁴⁰⁵ This one refers to the last draft of the E-Privacy Regulation texts of 6 March 2020.⁴⁰⁶ The purpose of the discussion paper is to reach agreement on the processing of electronic communication data. In view of the persistent disagreements between the Member States, the now following legislative process is supposed to take 2 more years.

Until then, the consequences for the various affected SPs must be assessed differently. For all services that are subject to the E-Privacy Directive, the fact remains that only the special rules of the E-Privacy Directive and the national laws based on it continue to apply (Art. 95 GDPR). For ISPs and advertisers, national tele media rights such as the German Telemedia Act are superseded by the GDPR.

With the E-Privacy Regulation not yet being enacted, legal uncertainty still exists. The EDPB has identified the following cases in which those affected by such data processing scenarios are confronted with the question of delimitation:

- where there is no interplay between the GDPR and the E-Privacy Directive because the matter falls outside of the scope of the GDPR;
- where there is no interplay between the GDPR and the E-Privacy Directive because the matter falls outside of the scope of the E-Privacy Directive; and
- where there is an interplay between the GDPR and the E-Privacy Directive because the processing triggers the material scope of both the GDPR and the E-Privacy Directive.

[...] There are many examples of processing activities which trigger the material scope of both the E-Privacy Directive and the GDPR. A clear example is the use of cookies. Case law of the Court of Justice of the European Union (CJEU) confirms that it is possible for processing to fall within the material scope of both the E-Privacy Directive and the GDPR at the same time⁴⁰⁷

⁴⁰⁵ Council of the European Union. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Presidency discussion paper, 2017/0003(COD), (6 July 2020).*

⁴⁰⁶ Council of the EU. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Presidency discussion paper, 2017/0003(COD), (6 July 2020).*

⁴⁰⁷ EDPB. *Opinion 5/2019 on the interplay between the E-Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, (12 March 2019). Paras. 21, 29*

The draft of the E-Privacy Regulation is nevertheless important to introduce specific rules for telecommunication services and Internet services as well as advertising services since such rules are missing in the GDPR but are to be regarded as necessary. In the future, work should be carried out on the delimitation from other Directives and Regulations as well as on sufficiently concrete and appropriate rules for specific processing purposes, if not in the text of the norm itself then at least in guidances or recommendations by the Commission or the EDPB.

3.4. General Data Protection Regulation

3.4.1. Subject-matter and objectives

The GDPR entered into force on 24 May 2016 and became applicable on 25 May 2018. It replaced Directive 95/46 and is, leaving aside the Charter, the current foundation of European data protection law. The GDPR “is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons”⁴⁰⁸ while “the processing of personal data should be designed to serve mankind.”⁴⁰⁹

After the GDPR was integrated into the EEA Agreement by the EEA Committee as “text with EEA relevance”, national legislation in each EEA State had to be amended in accordance with the GDPR before the act could have effect in the EEA Agreement.⁴¹⁰ Once three EEA States – apart from Switzerland – notified the conclusion of the parliamentary processes, the GDPR became applicable throughout the EEA States Norway, Island and Liechtenstein on 20 July 2018. These countries are therefore no longer “third countries” according to Arts. 44 ff. GDPR.

Its dual objective – data protection and free data flow, Art. 1(1) GDPR – originates from Art. 16(2) TFEU. The protection of natural persons against the processing of their personal data results from Art. 8 of the Charter and Art. 16(1) TFEU and is defined in more detail in Arts. 2 and 4 GDPR. The Union’s competence to harmonize data protection law according to Art. 16(2) TFEU was only added by the Treaty of Lisbon. The Directive 95/46 was based on Art. 95 TEU (now Art. 114 TFEU) as a regulation for the reduction of trade barriers, since different regulations in the Member States constituted obstacles to the exercise of fundamental freedoms; the GDPR also serves this objective.⁴¹¹ The goal of the free flow of personal data in the EU is achieved by harmonizing data protection provisions in Member States laws and ensuring a uniform interpretation of harmonized law. However, no normative decision in favor of improving the free flow of data at the expense of data protection can be inferred from the principle of the free flow of data. The principle of the free flow of data can therefore not be used as an argument at European level to justify a restriction of data protection. Such free flow of data is only guaranteed within the EU. It must however be ensured that the level of protection within the EU is not undermined by transferring personal data to a third country, Art. 44(2) GDPR.

According to Art. 1(2) GDPR, the GDPR protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The

⁴⁰⁸ GDPR, Recital 2

⁴⁰⁹ GDPR, Recital 4

⁴¹⁰ Arts. 7 and 102 of the EEA Agreement

⁴¹¹ GDPR, Recitals 9 and 13

processing of personal data thus affects not only Art. 8, but also Art. 7 of the Charter. This focus on a fundamental rights basis had been confirmed by the CJEU in various judgments. Furthermore, data processing can also indirectly affect the freedom of expression. Other fundamental rights are also affected by the GDPR insofar as they have to be reconciled with the right to the protection of personal data because of the GDPR's social function and the principle of proportionality.

Like it was also provided in Art. 1(2) Directive 95/46, the free flow of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data (Art. 1(3) GDPR). Thus, the goals of both Directive 95/46 and the GDPR are closely aligned. Nevertheless, as the GDPR has a direct binding effect for the Member States, it leads to a more harmonized approach and less inconsistent national compliance requirements. However, EU Members States' national provisions do not become obsolete, as the GDPR contains numerous "open clauses" in favor of a Member States' regulatory flexibility (for instance, Art. 6(2) GDPR). Member States are given – to some extent⁴¹² – the option of having their own rules relating to the processing of personal data. The aim of a harmonization of European data protection law is thus reached only to a slightly limited extent.

3.4.2. Scope

The GDPR applies to the processing of personal data by automatic means (e.g., a computerized system or database) and by other (non-automated) means that form part of a relevant filing system. The GDPR does not cover data that has no personal reference or data that relates only to legal persons. The protection of individuals should be technologically neutral, Art. 2(1) GDPR. Like Directive 95/46, the GDPR excludes several data processing activities, Arts. 2(2) and (3) GDPR. Data processing performed by national police forces and courts is not subjected to the GDPR, which sharpens its distinction towards the Law Enforcement Directive (LED).⁴¹³ Art. 2(3) GDPR clarifies that data processing by organs and bodies of the EU is not subject to the GDPR but to the proposed E-Evidence Regulation⁴¹⁴.

During the applicability of Directive 95/46, the Commission had become increasingly concerned that personal data processed outside the EU/EEA may not be adequately protected.⁴¹⁵ The GDPR therefore now has a broader extraterritorial reach than through Directive 95/46. Besides Art. 3(1) GDPR, which has due to the "establishment criterion" dual characteristics of territorial jurisdiction and extraterritorial jurisdiction, the application of the GDPR to a controller or processor established in a third country can also be determined when the processing of personal data of data subjects who are in the Union is related to "the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union (Art. 3(2)(a) GDPR); or the monitoring of the behavior of these data subjects as far as the behavior takes place within

⁴¹² Only in cases of Art. 6(1)(c) and Art. 6(1)(e) GDPR. Furthermore, the national provisions which are deriving from the GDPR must "ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX".

⁴¹³ LED // European Commission. (14 April 2016). *Joint Statement on the final adoption of the new EU rules for personal data protection*. http://europa.eu/rapid/press-release_STATEMENT-16-1403_de.htm.

⁴¹⁴ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). ("E-Evidence Regulation").

⁴¹⁵ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, COM(2012) 9 final, 10–11, (25 January 2012). P. 9–11.

the Union (Art. 3(2)(b) GDPR)". "Monitoring" may include tracking of an EU resident on the internet or the use of data processing techniques to profile individuals, their behaviors, or their attitudes. The question of what constitutes "offering" goods or services to EU residents is determined on a case-by-case basis.⁴¹⁶ In addition, Art. 3(3) GDPR regulates the application of the GDPR to processing at a location that is subject to the law of the EU Member States based on international law. Those responsible for the processing of personal data, which are based in third countries, will therefore have to examine whether they must comply with European data protection law.

In November 2021, the EDPB published guidelines on the relationship between Art. 3 GDPR and Chapter V of the GDPR. These guidelines concern on the one hand the significance of the new SDPC⁴¹⁷ in relation to the scope of applicability of the GDPR. In these guidelines, the EDPB found that a transfer to a third country must be safeguarded even if the recipient is subject to the GDPR due to Art. 3(2), because then local law of the third country can still undermine the level of protection of the GDPR. The EDPB noted that

This applies also in situations where the processing falls under Article 3(2) of the GDPR, in order to avoid that the protection provided by the GDPR is undermined by other legislation that the importer falls under. This may for example be the case where the third country has rules on government access to personal data that go beyond what is necessary and proportionate in a democratic society (to safeguard one of the important objectives as also recognized in Union or Member States' law, such as those listed in Article 23(1) GDPR). The provisions in Chapter V are there to compensate for this risk and to complement the territorial scope of the GDPR as defined by Article 3 when personal data are transferred to countries outside the EU."⁴¹⁸ [...] "It is worth underlining that controllers and processors, which are not established in the EU, may be subject to the GDPR pursuant to Article 3(2) for a given processing and, thus, will have to comply with Chapter V when transferring personal data to a third country or to an international organization."⁴¹⁹

The GDPR adopts the "one-stop-shop" mechanism. This means that data controllers and processors with activities in multiple EU countries are primarily subject to the authority of one "lead" SA, which supervises all processing activities of this data controller or processor. This aims to ensure more consistency in the application of data protection legislation throughout the EU. "Lead" in terms of jurisdiction could mean that under the GDPR one must distinguish "investigative jurisdiction" as a separate category of "jurisdiction" in a traditional sense. According to the judgment in the "Facebook fanpages case" this could mean that even when the German SA has jurisdiction to investigate complaints against Facebook (investigative jurisdiction), the German SA must primarily turn to the Irish SA when it comes to enforcement (traditional jurisdiction).⁴²⁰ Such a conclusion seems to be of elegant nature because users in Germany could then approach the German SA directly with no need to turn to the Irish SA, while at the same time Facebook can be ensured that any enforcement actions will primarily be brought in Ireland at Facebook's chosen seat in Europe.

⁴¹⁶ EDPB. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation*. (12 November 2019). P. 14.

⁴¹⁷ More on this therefore below, Chapter II, Section II.3.4.4.g.

⁴¹⁸ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Para. 3.

⁴¹⁹ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Para. 10.

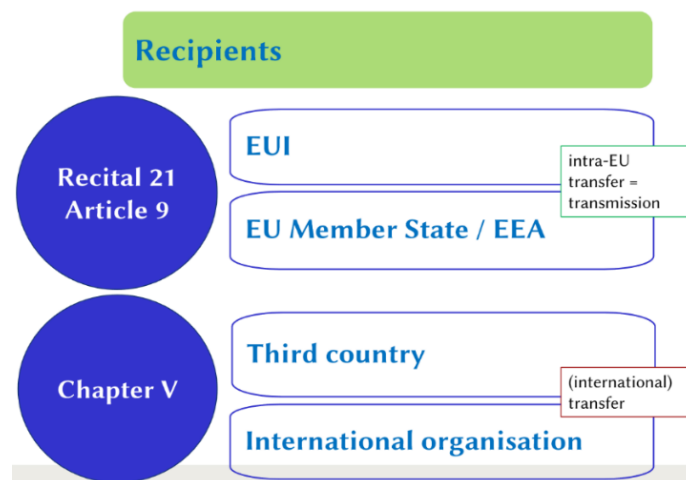
⁴²⁰ Facebook fanpages case.

3.4.3. Principles

The GDPR adopts the principles of data processing laid down in Art. 5 Directive 95/46 almost unchanged. Art. 5(1) GDPR has an equal tenor as to the conditions governing the admissibility of data processing. The provisions in Arts. 9(1), Art. 13(1), Art. 15(1), Art. 26 and 27, Art. 32 and 51 to 59 GDPR are conceptually similar. These regulations are specified, redesigned, or extended in the GDPR, but are not further developed in conceptual terms.

3.4.4. International data transfers

The provisions of Chapter V of the GDPR apply to any “transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization”, Art. 44 GDPR. The purpose of Chapter V of the GDPR is “to ensure that the level of protection guaranteed by the GDPR is not undermined when personal data are transferred to third countries or to international organizations”.⁴²¹ The GDPR offers instruments to guarantee this level of protection in scenarios of TFPD. Those are adequacy decisions, appropriate safeguards, and several derogations for specific data TFPD scenarios. The main differentiation of recipients of personal data is therefore made between a transfer to countries which provide an appropriate level of protection (Art. 45 GDPR) and to countries which do not grant such level (Arts. 46, 47, 49 GDPR).



Source: EDPS, “EUDPR: Conditions and Safeguards in International Transfers to Private Entities”⁴²²

“Third country” is understood as any country outside the EU/EEA. “International transfer” has been defined above⁴²³. “International transfer” is not defined explicitly in the GDPR, although Recital 101 of the GDPR, dealing with “General Principles for International Data Transfers” (which is an unofficial description), speaks of “flows of personal data to and from countries outside the Union and international organizations [...] when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organizations [...] including in cases of onward transfers of personal data from the third country or international organization”.

⁴²¹ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Para. 1.

⁴²² EDPS. *EUDPR: Conditions and Safeguards in International Transfers to Private Entities*. https://edps.europa.eu/system/files_en?file=2022-04/0167_2021-1047_01_redacted.pdf, (14 September 2021). P. 3.

⁴²³ Chapter I, Section II.5.3.

During a discussion between the Commission and the EDPB on the relationship between Art. 3 GDPR and Chapter V of the GDPR, the EDPB also addressed a more precise definition of “transfer of personal data to a third country or to an international organization” in its Guidelines 05/2021. In it, it suggested:

Since the GDPR does not provide for a legal definition of the notion “transfer of personal data to a third country or to an international organization”, it is essential to clarify this notion. The EDPB has identified the three following cumulative criteria that qualify a processing as a transfer: 1) A controller or a processor is subject to the GDPR for the given processing. 2) This controller or processor (“exporter”) discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor (“importer”). 3) The importer is in a third country or is an international organization, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.⁴²⁴

The data exporter may therefore be subject to the GDPR even if it is not established in the EU but is subject to the GDPR according to Art. 3(2) GDPR. A “disclosure” can happen through a transmission, but also through making-available of personal data. Whether the data importer is another controller (joint or not) or a processor is irrelevant. Also covered by the GDPR is the return of personal data by the processor in the EEA to the controller in a third country, as well as disclosure of these data by the processor to a sub-processor. Further, the EDPB noted that “if the sender and the recipient are not different controllers/processors, the disclosure of personal data should not be regarded as a transfer under Chapter V of the GDPR”⁴²⁵, which mainly concerns scenarios of employees accessing⁴²⁶ personal data stored at the employer’s seat in the EEA, without being a controller or processor.⁴²⁷ The third criterion “requires that the importer is geographically in a third country or is an international organization, but regardless of whether the processing at hand falls under the scope of the GDPR”⁴²⁸. This presumably requires a registered office in the third country. If all three of the above criteria are met, there is a transfer to a third country or to an international organization, “regardless of whether or not this importer is subject to the GDPR in respect of the given processing. As a consequence, the controller or processor in a “transfer” situation (according to the criteria described above) needs to comply with the conditions of Chapter V of the GDPR and frame the transfer by using the instruments which aim at protecting personal data after they have been transferred to a third country or an international organization.”⁴²⁹

⁴²⁴ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Para. 7.

⁴²⁵ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Para. 15.

⁴²⁶ It is still disputed whether the fact that servers belonging to responsables outside the EEA/EU are operated in the EEA/EU constitutes a third-country transfer. However, for providers that explicitly process personal data in the EU, but whose parent company is located in a third country, the reliability of such processors must still be specifically assessed again. See *Datenschutzkonferenz*. (31 January 2023). *Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 31. Januar 2023, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten*. https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf.

⁴²⁷ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Para. 14.

⁴²⁸ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Para. 18.

⁴²⁹ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Paras. 19–20.

a. Art. 44 GDPR (general principles for transfers)

Art. 44 GDPR facilitates the application of Chapter V of the GDPR by regulating general principles for transfers. Its first sentence provides that personal data may only be transferred to third countries or to international organizations if the controller and the processor comply with both the obligations laid down in Chapter V and all others of the GDPR. This is to ensure that the current “tools”⁴³⁰ through appropriate safeguards cannot be bypassed by transferring data to third countries. The second sentence makes it clear that the level of protection guaranteed by the GDPR must “not [be] undermined”, which is the result of the protection provided for in Art. 8 of the Charter and is intended to ensure the continuity of a high level of protection in the event of a data transfer to a third country. Thus, each transfer based on the safeguards set out in Chapter V of the GDPR must comply with the data protection principles in Art. 5 GDPR, be lawful in accordance with Art. 6 GDPR and comply with Art. 9 GDPR in case of the processing of special categories of data.

A permission must apply to the TFPD as such, together with all provisions of the GDPR, so the data transfer itself must be legitimate (first stage); and the provisions of Chapter V of the GDPR must be complied with, so the TFPD to a country outside EU/EEA must be permitted (second stage). Therefore, a “two-stage test” must be applied to all TFPD under Chapter V of the GDPR.

During the “first stage”, the assessment of the lawfulness of the processing starts with the question of whether effective consent of data subjects according to Art. 6(1)(a) GDPR in conjunction with Art. 7 GDPR exists or another permission of Art. 6(1) GDPR applies. The restriction of Art. 6(1)(f) GDPR is irrelevant in the present scenario, since it is not an authority but the (disclosing) company that wants to rely on a legal basis. It is only advisable in a few exceptional cases to base the transfer of personal data to US authorities and courts on the consent of the data subjects. First because it is usually difficult to ensure that the consent of all data subjects is available. In addition, the consent can be revoked at any time with future effect.

The transfer of personal data could also be based on Art. 6(1)(c) GDPR, if a legal obligation, to which the controller is subject, needs to be complied with. According to Art. 6(3) GDPR, only legal obligations based on Union law or the law of the Member States, to which the controller is subject, are in scope. Obligations under US law cannot be taken into consideration. The situation would be different if the requesting US authority, which may include a US litigation party or its lawyer, or a US court, would make an official request for assistance under “Mutual Legal Assistance Treaties” (MLATs) to a competent national authority in a Union Member State (e.g., in Germany, if the controller is subject to German jurisdiction because its main seat is located in Germany). In this case, the German authorities could oblige German companies to disclose data in accordance with national regulations, which is why Art. 6(1)(c) GDPR would then apply. The performance of a task which is in the public interest (Art. 6(1)(b) GDPR) cannot be considered as a legal basis since the restriction in Art. 6(3) GDPR also applies to Art. 6(1)(b) GDPR.

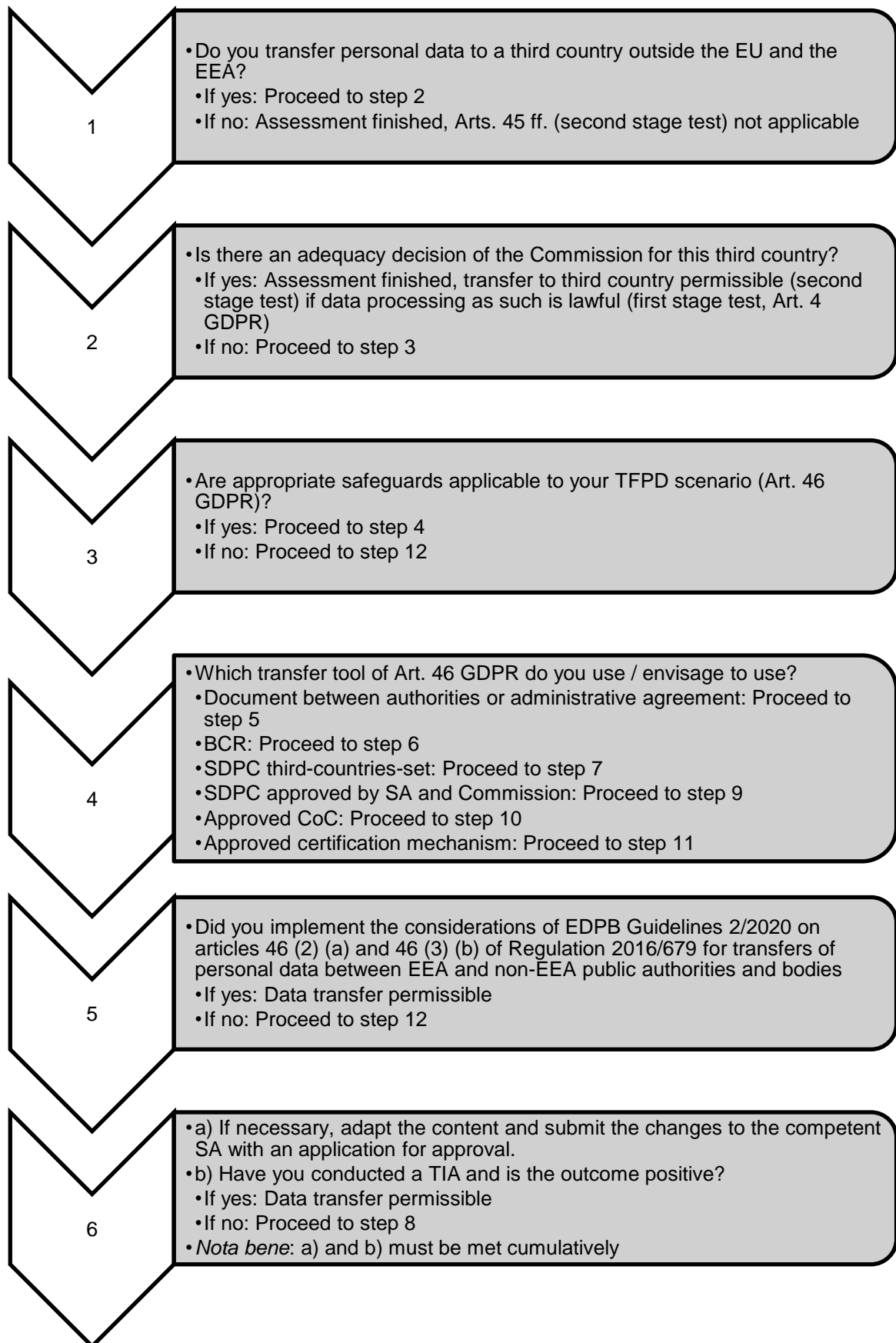
If the authority’s or court’s order to disclose data is not based on MLAT assistance, the balance between the interests of the controller and the data subjects are to be determined in accordance with Art. 6(1)(f) GDPR. A legitimate interest of the judiciary could lie in the facilitation or defense of a legitimate claim. Compliance with lawfully issued orders according to foreign law is a legitimate interest of the controller (in this

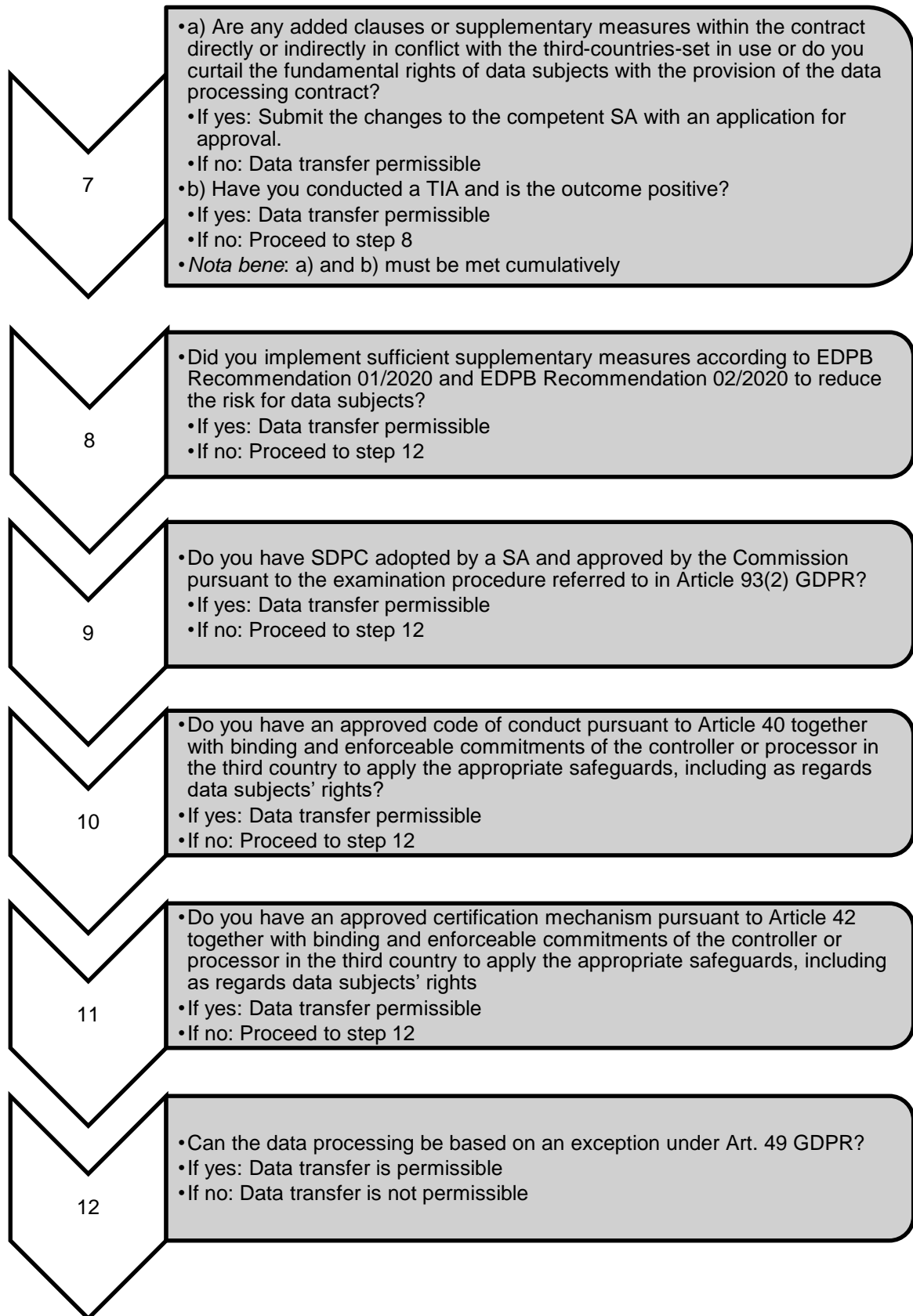
⁴³⁰ We hereby use the definition of the EDPB Recommendation 01/2020 (Version 2.0) in Para. 14: “A second step you must take is to identify the transfer tools you are relying on amongst those Chapter V GDPR lists and envisages.”

scenario the controller in Germany). Proportionality checks must consider the principle of necessity and the interests of the data subjects which means that only personal data that are objectively significant for the proceedings should be disclosed. The WP29 group therefore called for a filtering process in connection with a possible e-discovery process, in which initially only anonymized or pseudonymized data are disclosed and only the personal data required will be disclosed.⁴³¹ This approach is transferable to requests from US authorities related to criminal investigations. The restrictions on the processing of personal data on criminal convictions and offenses according to Art. 10 GDPR are not relevant, since the GDPR does not apply to data regarding acts of data subjects who commit a criminal offense. If special categories of personal data are to be disclosed in accordance with Art. 9(1) GDPR, the special circumstances of Art. 9(2) GDPR as well as any other EU Member State's national laws issued in accordance with Art. 9(4) GDPR must be applied.

The “second stage” assesses whether the TFPD to a third country is permitted. We present a scheme for the assessment of lawfulness of TFPD:

⁴³¹ WP29. *Working Document 01/2009 on pre-trial discovery for cross border civil litigation*, WP 158, (11 February 2009). P. 11.





b. Art. 48 GDPR (transfers or disclosures not authorized by Union law)

MNEs are often caught in between different jurisdictions, which leads to problems.⁴³² The latter have intensified since intelligence agencies and law enforcement agencies expanded their activities into the global digital space. US authorities may require access to data stored in the EU based on certain US laws,⁴³³ as the SWIFT agreement⁴³⁴ highlighted first, followed by the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism” (Patriot Act)⁴³⁵, the FISA, and the “Clarifying Lawful Overseas Use of Data Act” (Cloud Act)⁴³⁶. Based on US law, enforcement agencies could request MNEs to produce personal data of individuals stored on European servers without going through a MLAT⁴³⁷. Exemplarily, a US court had required in the so-called “*Microsoft Ireland case*”⁴³⁸ a US company to disclose personal data stored on computers located in Europe.

With Art. 48 GDPR, which must always be examined in addition to Arts. 45, 46, 47 and 49 GDPR, the European legislator takes a clear position in these cases of conflict. The TFPD to third country authorities cannot be based on judgments of a court or tribunal and any decision of an administrative authority of a third country. Rather, such transfers require a binding international agreement between the requesting third country and the Union or one of its Member States.⁴³⁹ In this respect, Art. 48 GDPR is designed to “prevent the circumvention of EU data protection law by the application of third country legal requirements”⁴⁴⁰, which will be subject to Chapter VIII, Section I.3.; and it “is designed to restrict the effect of extraterritorial assertions of jurisdiction by third country courts [...] and the best way to understand Article 48 is as a blocking statute⁴⁴¹ adopted to a data protection context”⁴⁴², which will be discussed in Chapter VIII, Section III.

c. Art. 45 GDPR (transfers on the basis of an adequacy decision)

Art. 45(1) GDPR provides for a system which corresponds to Art. 25(6) Directive 95/46 and authorizes the Commission to determine the adequacy of the level of protection. This removes possible different assessments in different Member States, which previously had led to obstacles in the legal practice of Member States.⁴⁴³ According to Art. 45 (1) GDPR, a transfer to a third country is permitted if the Commission has

⁴³² See also below Chapter VIII, Section III.

⁴³³ See also below Chapter III, Section II.1.2.

⁴³⁴ See also below Chapter II, Section II.4.1.

⁴³⁵ USA. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, H.R. 3162, Publ. L. No. 107–56, 115 Stat. 272, (26 October 2001). (“Patriot Act”).

⁴³⁶ USA. *CLOUD Act*, H.R. 4943, (2018). // See also below Chapter III, Section II.1.2.7.; the Cloud Act is codified in scattered sections of 18 U.S.C. and only addresses cooperation with regard to data stored abroad under the SCA [USA. *Stored Communications Act*, 18 U.S.C. Chapter 121, Paras. 2701–2713, (1986). (“SCA”)], not FISA.

⁴³⁷ Interestingly, MLATs are mentioned in Art. 48 GDPR, although MLATs which result in data transfers between enforcement authorities are anyway outside the scope of the GDPR.

⁴³⁸ See also below Chapter III, Section II.1.2.7.

⁴³⁹ Kuner, C. [Christopher]. (2020). Art. 48. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 825–840). Oxford University Press. P. 834–835.

⁴⁴⁰ Kuner, C. [Christopher]. (2020). Art. 48. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 825–840). Oxford University Press. P. 830.

⁴⁴¹ See also below Chapter VIII, Section III.

⁴⁴² Kuner, C. [Christopher]. (2020). Art. 48. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 825–840). Oxford University Press. P. 830.

⁴⁴³ Commission Staff Working Paper, Impact Assessment, SEC(2012) 72, p. 16 “a) Adequacy”, http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

determined – in a decision pursuant to Art. 288 (1) and (3) TFEU – that the level of protection in the recipient country is adequate. There are currently 14 adequacy decisions in force. On the other hand, the number of States that have data protection regulations has increased significantly.⁴⁴⁴ The Commission therefore announced that it will focus more on adequacy decisions in the future.⁴⁴⁵

The Commission can revoke an adequacy decision, Arts. 45(4) and 45(5) GDPR. The States for which an adequacy decision exists have therefore constantly to assess if they offer an adequate level of protection.

An adequacy decision usually refers to a third country as a whole but can also be restricted to certain areas or specific sectors. For reasons of legal certainty, the scope of partial adequacy decisions must be clearly defined based on objective criteria. Both the Safe Harbor decision and the decision on the Privacy Shield did not refer to the US as a whole, but only to companies which were committed to compliance with processing principles and were subject to supervision by the FTC or the Department of Transportation. The adequacy decision for Canada is limited to companies that are subject to the “Canadian Personal Information Protection and Electronic Documents Act”.⁴⁴⁶ TFPD based on such adequacy decisions do not require any further approval by the SA if such decision is still valid and applicable to the recipient country, Art. 45(1) GDPR. Many countries in the world do not have data protection legislation at all; an adequacy decision regarding these third countries or a sector within these countries pursuant to Art. 45(3) is therefore barred.

Art. 45(2) GDPR makes the adequacy analysis process more transparent because it defines the criteria to determine adequacy. Until *Schrems I*, it was uncertain if an adequate level of protection has to be “fully equivalent” to that of the Union or if reductions of the level of protection were permissible. The CJEU clarified in *Schrems I* that an adequate level of protection is given if it is “essentially equivalent” to that of the EU legal order.⁴⁴⁷ The CJEU nevertheless recognized that the measures to achieve such protection in the third country can differ from that in the EU. This limits the scope of the Commission decision finding because it does not allow the Commission to determine the adequacy of a third country for overriding political reasons. The CJEU also recalled that an adequacy decision is a measure of unilateral nature and not the result of negotiations (and concessions), such as between EU and US on the Privacy Shield and the EU-US DPF⁴⁴⁸. Regarding fundamental rights, the CJEU’s approach is consistent, because it effectively prevents the data protection level of the EU from being circumvented by transferring it to a third country or international organization. Accordingly, the CJEU does not grant the Commission room for maneuver on this issue and controls that the adequacy of a third country’s level of data protection cannot be based solely on political motives. A functional comparison between the legal practice of the third country and that of the EU is therefore important.

Recourse to Art. 49 GDPR as a legal base for a TFPD to a third country or international organization must remain an exception since they do not contain safeguards to

⁴⁴⁴ Greenleaf, G. [Graham] and Cottier, B. [Bertil]. (2020). 2020 Ends a Decade of 62 New Data Privacy Laws. *Privacy Laws & Business International Report*, Vol. 163, 24–26.

⁴⁴⁵ European Commission. *Commission communication on the exchange and protection of personal data in a globalized world*, COM(2017) 7 final, (10 January 2017). P. 9.

⁴⁴⁶ European Commission. (4 January 2002). *C2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)*, OJ L 2, 13–16.

⁴⁴⁷ *Schrems I*. Para. 73.

⁴⁴⁸ See Chapter IX, Section II.1.; and Chapter IX, Section III.3.

guarantee an adequate level of protection. In the absence of a decision pursuant to Art. 45(3), the task to make such TFPD permissible is covered by the appropriate safeguards set out in Art. 46 GDPR. This approach reaches its limits if there are deficits based on the legal system of the third country to which the recipient is subject. If a transfer is already permitted under Art. 45 GDPR, European data exporters may freely choose between both alternatives (Arts. 45 or 46) and are not obliged to rely on a (eventually invalid) adequacy decision of the Commission. This practice of parallel applicability was also common under Directive 95/46, where MNEs were subject to the Safe Harbor program or its successor, Privacy Shield, but also offered the conclusion of SDPC. It would also be contradicting the purpose of Arts. 44 ff. GDPR if a “double compliance” with the data protection level in a third country would be inadmissible. It may also make sense for a data exporter not to rely on an adequacy decision if it has doubts about its legality.

In the case of BCR, the goal is to create internationally valid guarantees for the handling of personal data within a MNE; this would not be possible if branches and subsidiaries of this MNE, to which a transfer was already permitted on the basis of an adequacy decision, could not participate.

Art. 45(4) and (5) GDPR require the Commission to monitor the adequacy of the level of protection in the third country on an ongoing basis in accordance with Art. 45(3) GDPR. Existing decisions under Art. 25(6) of Directive 95/46 remain in force after the entry into force of the GDPR (Art. 45(9) GDPR) but are subject to the Commission’s supervision and revocation obligations under Art. 45(4) and (5) GDPR).

d. Art. 46(1) GDPR (principle of prohibition for transfers)

Systematically, Chapter V of the GDPR provides for a principle of prohibition of a transfer with a reservation of permission.⁴⁴⁹ Therefore, transfers to third countries are generally not permitted unless one of the reasons for permission in Arts. 44 ff. GDPR applies.

The same level of protection must be guaranteed for data subjects in the case of transfers based on tools within the meaning of Art. 46 GDPR as in the case of transfers based on an adequacy decision according to Art. 45 GDPR. “In the absence of an adequacy decision, data transfers to third countries could be permissible if the controller or processor take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject”.⁴⁵⁰ Recital 108 of the GDPR requires that

those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country.⁴⁵¹

⁴⁴⁹ Although Roßnagel pointed out – in our view unjustifiable – that according to the Charter and the GDPR, data processing is not prohibited per se, but the legislator is called upon to determine which processing is desirable and which is not. Roßnagel found that the wording of Art. 9(1) GDPR might indicate that the GDPR does not determine a “prohibition principle” but rather a “permission reservation”, otherwise Art. 9(1) GDPR would be superfluous if the GDPR were based on a general ban on processing. See Roßnagel, A. [Alexander] (2019). Kein “Verbotsprinzip” und kein “Verbot mit Erlaubnisvorbehalt” im Datenschutzrecht. *Neue Juristische Wochenschrift*, 72(1), 1–5. P. 2 f.

⁴⁵⁰ Recital 108 of the GDPR

⁴⁵¹ Recital 108 of the GDPR

The “minus” (in a sense of lack) in the level of protection in the third country or international organization could then be compensated by the “plus” through safeguarding measures by those responsible for the transfer.

e. Art. 46(2) (a) GDPR (legally binding and enforceable instrument between public authorities or bodies as appropriate safeguard)

Those responsible for the transfer may provide appropriate safeguards – without requiring specific authorization from a SA – through the use of one of the transfer tools listed under Arts. 46(2) or (3) GDPR. The safeguards in Art. 46(2) and (3) GDPR have in common that they are provided by means of contractual or contract-like agreements by those responsible for the data transfer, and thus have “*inter partes*” effects. The difference between Art. 46(2) and (3) GDPR is that the latter covers only those safeguards that are not “legally binding”, and in this respect “authorization by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding”.⁴⁵²

Art. 46(2)(a) GDPR requires an “instrument” that is legally binding and enforceable, without further explaining this term. Recital 108 of the GDPR explains that

transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organizations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects.⁴⁵³

Administrative agreements without a legally binding character or enforceability are expressly excluded from Art. 46(2)(a) GDPR; in such cases, however, a transfer according to Art. 46(3)(b) GDPR could still be considered. Both instruments included in Arts. 46(2)(a) and 46(3)(b) GDPR will be hereinafter called “international agreements between public bodies”. This structure between Art. 46(2) and (3) GDPR is a change compared to the legal situation under Directive 95/46 and simplifies the application of the safeguards. Procedures regulated in the GDPR (e.g., Art. 93 GDPR), within which a content-related examination by the SA or the Commission takes place, guarantee that an adequate level of protection is ensured during the design of the safeguards.

The GDPR does not define what constitutes a “public authority or “public body”. With respect to public bodies in third countries, the notion is to be determined under domestic law; accordingly, public bodies can include government authorities at different levels (e.g., national, supranational and local authorities) and other bodies governed by public law (e.g., executive agencies).⁴⁵⁴ Art. 46(2)(a) GDPR applies to all instruments concluded after 24 May 2016 (Art. 96 GDPR), which may be of bilateral or multilateral nature.⁴⁵⁵ Member States may conclude those, “as far as such agreements do not affect

⁴⁵² Recital 108 of the GDPR

⁴⁵³ Recital 108 of the GDPR

⁴⁵⁴ EDPB. *Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublic_bodies_v2_en.pdf, (15 December 2020). P. 5.

⁴⁵⁵ EDPB. *Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublic_bodies_v2_en.pdf, (15 December 2020). P. 6.

this Regulation [the GDPR] or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects”⁴⁵⁶.

The scope of Art. 46(2)(a) GDPR raises the question to what extent public authorities and bodies have the option of entering legally binding obligations towards another public body in a third country; because to maintain the administrative legal order, only a State as the ultimate holder of the hierarchy of norms should be allowed to do so. Arts. 216 ff. TFEU offer the possibility to conclude binding international agreements in certain cases to the EU. Legally binding and enforceable is such an agreement then, in view of Art. 46(1) GDPR, if the data subjects can enforce the rights granted to them in the agreement’s provisions. The document must therefore give them effective administrative or judicial remedies as well as the right to compensation.⁴⁵⁷ The EDPB has elaborated a list of minimum safeguards to be included in international agreements between public bodies falling under Art. 46(2)(a) or Art. 46(3)(b) GDPR.⁴⁵⁸

Authorities including public bodies in the Member States that wish to transfer personal data from the Union enjoy a certain preferential treatment. The background to this is that, due to their commitment to the law, in particular to the Charter (Art. 51 of the Charter), it can be expected that they will comply with the fundamental rights and freedoms of data subjects. As for transfers of personal data carried out between public bodies, specific guidance is therefore provided by the EDPB.⁴⁵⁹

f. Art. 46(2)(b) GDPR (BCR as appropriate safeguard)

In contrast to Directive 95/46, the GDPR now expressly recognizes BCR as a tool in Arts. 46(2)(b) and 47 GDPR. Arts. 4(19) and 4(20) GDPR as well as Recital 110 of the GDPR do not explicitly exclude certain types of “group of undertakings” as long as they exercise a “joint economic activity”. However, BCR in practice are not used for TFPD to recipients outside these types, as BCR are primarily a matter of interest for a MNE.

Despite some position papers from SAs, there are – different to the SDPC tool – yet no pre-approved BCR templates.⁴⁶⁰ Therefore, those responsible for the data transfer must design the content of the BCR for the specific TFPD scenario. The details of the obligations in BCR finally depend on the negotiations of the responsible entities with the SA that approves the BCR. Under the GDPR, at least the minimum content for BCR is now specified. They must therefore (i) be legally binding and apply to all relevant members of the data controller group and be enforced by these members, (ii) expressly transfer enforceable rights to the data subjects with regard to the processing of their personal data and (iii) respect the rights set out in Art. 47(2) GDPR. In this context, the “one-stop-shop” mechanism introduced by the GDPR results in the authorization being carried out by the SA responsible for the European head office of the MNE according to the consistency procedure set out in Art. 63 GDPR.

⁴⁵⁶ Recital 102 of the GDPR

⁴⁵⁷ Recital 108 of the GDPR

⁴⁵⁸ EDPB. *Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublic_bodies_v2_en.pdf, (15 December 2020). P. 6 ff. // These minimum safeguards will be analyzed in detail in Chapter IX, Section III.2., which will deal with the comparison of core data principles in other legal frameworks at global level.

⁴⁵⁹ EDPB. *Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublic_bodies_v2_en.pdf, (15 December 2020).

⁴⁶⁰ WP29. *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, WP 256, (6 February 2018).

If a MNE introduces BCR, all legal entities of this enterprise that are not based in the Union can also commit themselves to the BCR, which would then encompass all TFPD within the group. Such groups must implement different tools for transfers to non-group companies. If a group of companies has introduced BCR that require recipients of onward transfer(s) to accept the same BCR regarding the data transfer in question, it could be difficult to enforce this in practice, as suppliers and other third Parties might want to first check the rules set out in those BCR before being bound by them. In addition, controllers could be reluctant to roll out BCR globally because they might contain obligations under Union law which they might consider inappropriate or even unfavorable for TFPD from other regions or countries where such group has legal entities. The CJEU did not comment on possible contractual arrangements as safeguards in *Schrems II*. There is therefore yet no clear indication if the requirements from *Schrems II* must be observed also for other transfer tools according to Art. 46(2) GDPR – such as BCR. BCR have a binding effect on the contract Parties (“*inter partes*”), similar as SDPC. The principles established by the CJEU in *Schrems II* should therefore also be observed here and companies should check whether there is an adequate level of protection in the recipient country and, if this is not the case, use supplementary measures. In cases in which SDPC cannot be effectively agreed upon and a TIA shows an unacceptable result, BCR should not be considered either because they would not change the fact to not uphold the required level of protection in the third country. Analogous to “SDPC+”⁴⁶¹ it might then be feasible to envisage the drafting of “BCR+”, meaning to include supplementary measures therein. However, due to abovementioned difficulties associated with BCR, BCR+ compared to SDPC+ appear impractical.

g. Art. 46(2)(c) GDPR (SDPC adopted by the Commission as appropriate safeguard)

Art. 46(2)(c) and (d) GDPR recognize SDPC as appropriate safeguards. SDPC are binding for the Member States and therefore also for their SAs, Art. 288 (4) TFEU.⁴⁶² SDPC are at best to be adopted unaltered. Nevertheless, the GDPR now expressly provides that further clauses or supplementary measures can be added to the SDPC as long as these are neither directly nor indirectly in conflict with the provisions of the SDPC.⁴⁶³ Companies may thus change the SDPC or draft their own data processing contracts, but these alterations are then subject to the laws of the respective Member State and require further reporting obligations and approvals from the SAs. A new element compared to Directive 95/46 is that a data transfer, when using unaltered SDPC, does no longer require approval by the SA. Nevertheless, if authorities have doubts about the effectiveness of an adequacy decision, they are obliged to submit it to a national Member State court, which can then submit a referral to the CJEU.

A multi-party contract is often favored by groups that want to map as many data transfers as possible within the group in one comprehensive contract. In such cases it could be difficult to assess whether the result is a significant alteration of the SDPC (and therefore would need an approval by the competent SA). The inclusion of SDPC within a multi-party contract does not itself represent a significant change to the SDPC, if this contract specifies which data are transferred from which data exporter to which data importer, and whether the data importer is a controller or a processor. Moreover, the individual data flows and the roles of those involved must be clear. Instead of making use of a so-

⁴⁶¹ It could be feasible to reach a required level of protection through a data processing contract that includes the guarantees set out in the currently applicable SDPC but goes even beyond those by for example including a statement of the type of data processed and the scope of the intended processing; this mechanism of increased protection through supplementary measures would then be a so-called “SDPC+”

⁴⁶² Provisions of these three Sets analyzed above in Chapter II, Section II.3.1.

⁴⁶³ Recital 109 of the GDPR

called “ad hoc clause” (Art. 46(3)(a)), the conclusion of a SDPC between an EU controller as the data exporter directly with the sub-processor (located in a third country with no adequate level of protection) could be an option to avoid obligatory approval by a SA. The main processor in the Union could even contract with the sub-processor – if he has been granted that power - in the name and on behalf of the controller. The main processor could also join the SDPC between controller and sub-processor, the main processor would then exercise the control powers of the controller against the sub-processor. This administrative effort could at least be somewhat reduced if the group would be able to centrally obtain powers from all subsidiaries. But it also could occur that subsidiaries of that group refuse to execute the contracts because the implementation of measures is not enforceable at their local level. Even more, it could be a challenge to get legal entities, that do not belong to the group, to sign the SDPC. As other countries are increasingly enacting or updating their data protection laws and introducing additional or different requirements, a MNE therefore could tend to work with centralized powers to facilitate legal certainty in case of changes in national laws.

The Commission had announced that it would consider the adoption of more sector-specific SDPC that are tailored to the circumstances of certain economic sectors, such as healthcare and IT outsourcing.⁴⁶⁴ The Commission published those drafts on 12 November 2020:

- Draft Commission Implementing Decision and its draft Annex on SDPC for the transfer between controllers & processors located in the EU (“controller-processor-draft-set”);⁴⁶⁵
- Draft Commission Implementing Decision and its draft Annex on SDPC for the transfer of personal data to third countries pursuant to the GDPR (“third-countries-draft-set”).⁴⁶⁶

On 4 June 2021, the Commission adopted them as final version:

- Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (“controller-processor-set”);⁴⁶⁷
- Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (“third-countries-set”).⁴⁶⁸

The controller-processor-set has no predecessors. The third-countries-set replaced the existing SDPC for international transfers, which were adopted based on Directive 95/46,

⁴⁶⁴ European Commission. *Commission communication on the exchange and protection of personal data in a globalized world*, COM(2017) 7 final, (10 January 2017). P. 10–11.

⁴⁶⁵ European Commission. (2020). *Data protection - standard contractual clauses between controllers & processors located in the EU (implementing act)*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Data-protection-standard-contractual-clauses-between-controllers-processors-located-in-the-EU-implementing-act_en.

⁴⁶⁶ European Commission. (2020). *Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act)*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act_en.

⁴⁶⁷ European Commission. *Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council*, C/2021/3972, OJ L 199, 18–30, (7 June 2021). (“controller-processor-set”).

⁴⁶⁸ European Commission. *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, C/2021/3701, OJ L 199, 31–61, (7 June 2021). (“third-countries-set”).

to bring them in line with GDPR requirements⁴⁶⁹, with *Schrems II*⁴⁷⁰, and to better reflect the widespread use of new and more complex processing operations often involving multiple data importers and exporters.⁴⁷¹

The third-countries-set came into force on 27 June 2021. After 27 September 2021, the “old” set can no longer be used for new contracts. However, it will continue to be considered “appropriate” for an additional 15 months if the regulatory subject matter of those contracts remains unchanged, and the “old” set was previously “appropriate.” As of 27 December 2022, the use of the “old” set does no longer provide the necessary adequate safeguards for a data transfer to a third country. Since then, it must therefore be replaced by the “new” set.

In *Schrems II*, the CJEU had to answer the question of which aspects are to be considered when determining whether the use of SDPC provides for an adequate level of protection according to Arts. 46(1) and 46(2)(c) GDPR.⁴⁷² The CJEU ruled that Art. 44 GDPR is to be interpreted in the light of all articles of Chapter V of the GDPR, which is why the level of protection created by all rules of the GDPR must not be undermined.⁴⁷³ An essentially equivalent level of protection is sufficient, an identical level is not required; the CJEU hereby repeated its opinion of *Schrems I* in *Schrems II*.⁴⁷⁴ When assessing the level of protection, the contractual rules between the controller or the processor in the EU, and the recipient in the third country or at an international organization, as well as the relevant elements of the legal system of the third country or the international organization, including the access by authorities there to the transferred personal data must be taken into account.⁴⁷⁵

The CJEU also decided whether national SAs can suspend or prohibit a data transfer based on the SDPC tool if the SAs are of the opinion that the European level of protection is not being achieved, or whether these powers for the SAs are limited to exceptional cases.⁴⁷⁶ The CJEU found that the SAs not only have the right to monitor compliance with the GDPR but are obliged to suspend or prohibit a transfer of personal data if they believe that the SDPC cannot be complied with for that transfer.⁴⁷⁷ This cannot be restricted either, meaning that this obligation does not only relate to individual cases.⁴⁷⁸ However, a possible adequacy decision for the third country, against which no contrary decision can be made, should be taken into account.⁴⁷⁹

Furthermore, the CJEU expressly confirmed SDPC being an appropriate safeguard for international data transfers, although within a SDPC tool the criticized data protection

⁴⁶⁹ European Commission. *Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, Document Ares(2020)6654429. Recital 2.

⁴⁷⁰ “level of protection essentially equivalent to that which is guaranteed within the European Union”, *Schrems II*. Para. 96 // “[s]ince by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries [...] it may prove necessary to supplement the guarantees contained in those standard data protection clauses”, *Schrems II*. Para. 132 // See also European Commission. *Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, Document Ares(2020)6654429. Recital 18.

⁴⁷¹ European Commission. *Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, Document Ares(2020)6654429. Recital 6.

⁴⁷² *Schrems II*. Para. 90

⁴⁷³ *Schrems II*. Paras. 92 and 93

⁴⁷⁴ *Schrems I*. Para. 73 // *Schrems II*. Para. 96

⁴⁷⁵ *Schrems II*. Para. 104

⁴⁷⁶ *Schrems II*. Para. 106

⁴⁷⁷ *Schrems II*. Paras. 108 and 113

⁴⁷⁸ *Schrems II*. Para. 115

⁴⁷⁹ *Schrems II*. Paras. 116 and 118

weaknesses inherent to the US framework would persist.⁴⁸⁰ SDPC must then still guarantee an adequate level of protection. SDPC can provide such level unless the legal situation in the recipient country allows its authorities to intervene with the rights of the data subjects affected by the data transfer.⁴⁸¹ Unlike in the case of an adequacy decision, the Commission does not assess the level of protection in the recipient country but puts this duty now on the shoulders of those responsible for the data transfer.⁴⁸² The EU data exporter, respectively its EU data processor, has now the obligation to conduct a TIA to find out whether personal data within a transfer, which is based on SDPC, are essentially equally protected in the third country, which does not include the duty to evaluate the entire legal system of the third country but of those provisions that are applicable to the transferred personal data;⁴⁸³ the latter encompasses not only the processing at the recipient's side but rather the entire transfer route of personal data. This TIA must determine whether the data subjects in the third country have enforceable rights and effective legal remedies. Companies are therefore "now obliged to undertake "mini-adequacy" findings for each of their data transfers (as they are required to assess the laws of the country of destination themselves and on that basis, decide which safeguards would be the most appropriate). This is simply not feasible in practice".⁴⁸⁴ Since the TIA must be carried out for each individual case,⁴⁸⁵ the results for one and the same country may well be different. In view of the access to personal data by US authorities, which became public through the Snowden revelations, an appropriate level of protection in the case of the US is probably not ascertainable; the assessment of the transfer would then lead to a negative TIA result.

When conducting the assessment, it must be considered that the SDPC, "due to their contractual nature, [...] cannot bind the public authorities of third countries, since they are not party to the contract."⁴⁸⁶ SDPC have only "*inter partes*" effect and thus no influence on the substance of the legal system in the third country and cannot constructively guarantee a level of protection. The SDPC therefore do not protect against local agencies' access whilst transferring personal data, since the intermediaries used are not party to the contract. "Consequently, data exporters may need to supplement the guarantees contained in the SDPC with supplementary measures to ensure compliance with the level of protection required under EU law in a particular third country."⁴⁸⁷ The TIA must be fulfilled before commencing the transfer and be documented in addition to an assessment of any further compensatory measures (Art. 5 (2) GDPR).⁴⁸⁸

If the data recipient cannot fulfill the obligations of the SDPC due to the legal situation in the recipient's country, it must not only inform the responsible body based in the EU, but also refrain from transferring the data.⁴⁸⁹ If it is evident that the data importers are subject to US laws that make it impossible for those responsible for the data transfer to comply with the SDPC, it could then be feasible to reach the required level of protection through supplementary measures. The Commission pointed out that it "does not prevent the Parties from including the standard contractual clauses laid down in this Clauses in a wider contract, and to add other clauses or additional safeguards provided that they do

⁴⁸⁰ Schrems II. Para. 123

⁴⁸¹ Schrems II. Para. 126

⁴⁸² Schrems II. Para. 130

⁴⁸³ Schrems II. Para. 134

⁴⁸⁴ Voss, A. [Axel]. (25 May 2021). *Position Paper on Fixing the GDPR: Towards Version 2.0*. <https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf>. P. 31 // Axel Voss is Member of the European Parliament

⁴⁸⁵ Schrems II. Para. 134.

⁴⁸⁶ EDPB Recommendation 01/2020 (Version 2.0). Recital 4.

⁴⁸⁷ EDPB Recommendation 01/2020 (Version 2.0). Recital 4 // See also Schrems II. Recital 109.

⁴⁸⁸ Schrems II. Paras. 141 ff.

⁴⁸⁹ Schrems II. Paras. 135 ff.

not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects”⁴⁹⁰.

The CJEU did not specify what supplementary measures are, which was a reason for uncertainty among companies and data subjects and put a tension on ongoing data-driven business. The EDPB therefore adopted Recommendations 01/2020 (Version 1.0) on such measures that should supplement transfer tools to ensure compliance with the EU level of protection.⁴⁹¹ As the EU Commission issued new SDPC in June 2021,⁴⁹² the EDPB Recommendation 01/2020 was updated to Version 2.0 by the EDPB on 18 June 2021. Their aim is “to help exporters (be they controllers or processors, private entities or public bodies, processing personal data within the scope of application of the GDPR) with the complex task of assessing third countries and identifying appropriate supplementary measures where needed”.⁴⁹³ In doing so, the EDPB seeks a consistent application of the GDPR and the CJEU’s ruling across the EEA.

EDPB Recommendation 01/2020 (Version 2.0) contains several examples of supplementary measures, in particular of technical nature. They also describe specific scenarios for which effective technical measures might be found. The EDPB believes that, e.g., for cloud-based services which process personal data, the most important point is an adequately strong encryption, for which only the data exporter and not the data importer have the encryption key. The Austrian SA recently ruled some technical-organizational measures useless – which Google had argued to be sufficient privacy protection – when it comes to potential access to personal data by US authorities. The Austrian SA found that

as far as the technical measures are concerned, it is also not recognizable - and was not explained comprehensibly by the respondents - to what extent the protection of communication between Google services, the protection of data in transit between data centers, the protection of communication between users and websites or an ‘on-site security’ actually prevent or restrict the access possibilities of US intelligence services on the basis of US law.⁴⁹⁴

The decision is based on the first of 101 complaints filed by NOYB⁴⁹⁵ following *Schrems II*. This SA determined therein that “configuration abilities for customers, including truncating IP addresses, are insufficient to prevent re-identification, potentially by Google or the U.S. government [and] supplementary measures implemented by Google, including government access transparency reports and encryption of data, were insufficient”⁴⁹⁶. On 11 January 2022, the EDPS issued a similar decision, stating that the European Parliament’s use of Google Analytics on a COVID-19 test booking website

⁴⁹⁰ European Commission, Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Document Ares(2020)6654686, Annex, Clause 1(c)

⁴⁹¹ EDPB. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 1.0*, (10 November 2020), https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransfer_stools_en.pdf. (“EDPB Recommendations 01/2020 (Version 1.0)”).

⁴⁹² See below within this Section.

⁴⁹³ EDPB Recommendation 01/2020 (Version 2.0). P. 3.

⁴⁹⁴ *Datenschutzbehörde der Republik Österreich*. (22 December 2021). *Decision of 22 December 2021*. https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf.

⁴⁹⁵ “NOYB - European Center for Digital Rights” is a Vienna-based non-governmental organization dedicated to the enforcement of data protection within the European Union. It was founded in 2017 by Maximilian Schrems, among others. See also <https://noyb.eu>.

⁴⁹⁶ Bryant, J. [Jennifer]. (20 January 2022). *Austrian DPA’s Google Analytics decision could have “far-reaching implications”*. <https://iapp.org/news/a/far-reaching-implications-anticipated-with-austrian-dpas-google-analytics-decision>.

launched in September 2020 violates the GDPR.⁴⁹⁷ Moreover, the French SA⁴⁹⁸, the Dutch SA,⁴⁹⁹ the Italian, and the Danish SA⁵⁰⁰ were investigating complaints on the use of Google Analytics. The Italian SA⁵⁰¹ found that users' IP addresses, browser and operating system information, and more was transferred to the United States, a country without an adequate level of protection. The authority gave companies 90 days to rectify issues.⁵⁰² The Danish SA became the latest EU authority to order a halt on the use of Google Analytics for data transfers to the US without supplementary measures and advised Danish businesses to assess whether their possible continued use of the tool is within the framework of the GDPR.⁵⁰³ IAPP reported therefore, that "if taken literally, this turns *Schrems II* from a data export law into a data localization law, effectively permitting processing by organizations only within the EU – in stark contradiction to the GDPR's recognition that flows of personal data to and from countries outside the Union and international organizations are necessary for the expansion of international trade and international cooperation"⁵⁰⁴.

The EDPB outlines six steps that data exporters should take to comply with their accountability:

Step 1) Analysis of data transfers to third countries (Data mapping)

Data exporters need to be aware of the TFPD they are undertaking to third countries. The entire processing chain must be considered (also onward transfers) as well as potential access options (remote access) from third countries by affiliated group companies, even if the personal data are processed within the EEA.⁵⁰⁵ Particularly the due diligence regarding possible onward transfers complicates Step 1) in practice.⁵⁰⁶ Companies that keep records of processing activities should be able to conduct this far easier as others, since these records indicate whether transfers are made to third countries, Art. 30(1)(e) GDPR. A data controllers' information obligation may also contain references to third country transfers, Arts. 13(1)(f), 14(1)(f) GDPR. It is recommended

⁴⁹⁷ EDPS. *Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament*, https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf, (11 January 2022).

⁴⁹⁸ *Commission Nationale de l'Informatique et des Libertés*. (10 February 2022). *Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply*. <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>. // This SA further released an undisclosed number of compliance notices to companies over data transfers carried out through Google Analytics, granting a 30-day compliance period. See *Commission Nationale de l'Informatique et des Libertés*. (7 June 2022). *Questions-réponses sur les mises en demeure de la CNIL concernant l'utilisation de Google Analytics*. <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/questions-reponses-sur-les-mises-en-demeure-de-la-cnil-concernant-lutilisation-de-google-analytics>.

⁴⁹⁹ *Autoriteit Persoonsgegevens*. (2022). *Bekijk binnen het onderwerp Cookies*. <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#hoe-kan-ik-bij-google-analytics-de-privacy-van-mijn-websitebezoekers-beschermen-4898>.

⁵⁰⁰ *Datatilsynet*. (19 January 2022). *Afgørelse om brug af Google Analytics fra det østrigske datatilsyn*. <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jan/afgoerelse-om-brug-af-google-analytics-fra-det-oestrigske-datatilsyn>.

⁵⁰¹ *Garante per la protezione dei dati personali*. (23 June 2022). *Google: Garante privacy stop all'uso degli Analytics. Dati trasferiti negli Usa senza adeguate garanzie*. <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782874#english>.

⁵⁰² Bryant, J. [Jennifer]. (28 June 2022). *Google Analytics enforcement fallout: 'Cry and pray'*. <https://iapp.org/news/a/google-analytics-enforcement-fallout-cry-and-pray>.

⁵⁰³ *Datatilsynet*. (21 September 2022). *Brug af Google Analytics til webstatistik*. <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/brug-af-google-analytics-til-webstatistik>.

⁵⁰⁴ Bryant, J. [Jennifer]. (20 January 2022). *Austrian DPA's Google Analytics decision could have "far-reaching implications"*. <https://iapp.org/news/a/far-reaching-implications-anticipated-with-austrian-dpas-google-analytics-decision>.

⁵⁰⁵ EDPB Recommendation 01/2020 (Version 2.0). Paras. 8–13.

⁵⁰⁶ Georgescu, F. [Florin]. (18 November 2021). *PrivacyConnect*. Zurich. <https://event.on24.com/wcc/r/3380148/72924565275FB73E289A885729C0DF08?mode=login&email=philipp.fischer@ip.mpg.de>.

that data exporter check the relevant contracts and, if necessary, contact the contractual partner or the manufacturer for clarification.⁵⁰⁷

Step 2) Identification of the transfer tools used

If Art. 49 GDPR cannot be applied, data exporters must identify which of the transfer tools named in Art. 46 GDPR could be used and whether these tools are still valid. This procedure lies within the aforementioned “second stage” of the check of permissibility of the data transfer to a third country.⁵⁰⁸

Step 3) Assessment of the effectiveness of the transfer tools (TIA)⁵⁰⁹

The third step is directed to the question whether the transfer tool used offers effective protection in light of all circumstances of the transfer.⁵¹⁰ Data exporters are requested, if necessary with the help of the data importer, to assess whether the law or the practices of the third country could threaten the effectiveness of the transfer tool used.⁵¹¹ CJEU and EDPB thus expect data exporters to carry out a comprehensive legality assessment based on the elements of Art. 45(2) GDPR. TIA therefore ultimately becomes alike a Commission’s examination of the appropriate level of protection in a third country prior to issuing an adequacy decision.⁵¹² The complexity of the TIA can also be exemplified by this graphic, which is one of many published by businesses trying to approach compliance after *Schrems II* for multiple TFPD.

⁵⁰⁷ See also *Schrems II*. Para. 134.

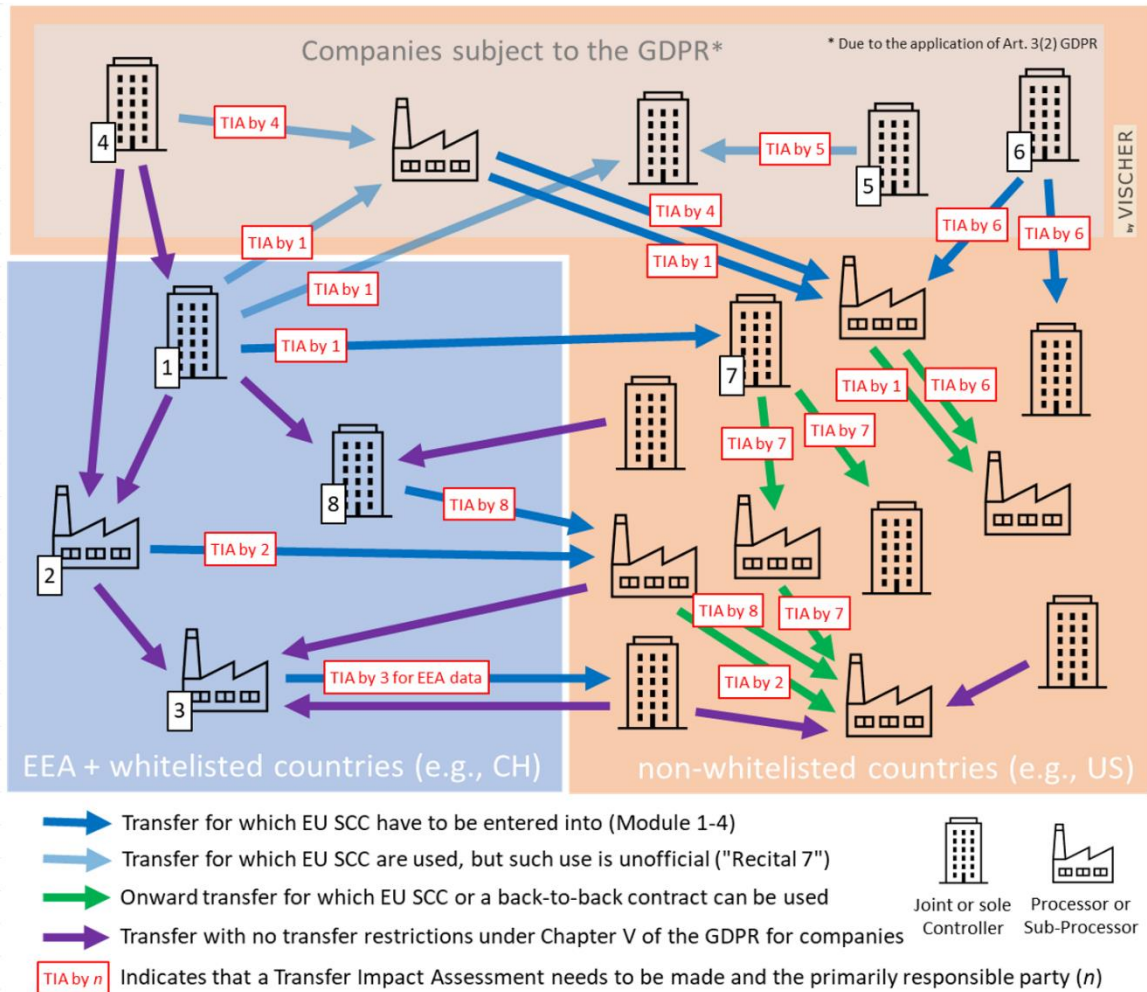
⁵⁰⁸ See above Chapter II, Section II.3.1. // Recalling that the “first stage” corresponds to an assessment if the data processing activity as such (a transfer inside EEA) is permissible, “second stage” assesses then lawfulness based on Art. 44 ff. GDPR (transfer to third country outside EEA).

⁵⁰⁹ This step was already included in EDPB Recommendations 01/2020 (Version 1.0 as well as Version 2.0).

⁵¹⁰ EDPB Recommendation 01/2020 (Version 2.0). Para. 28: “The selected Article 46 GDPR transfer tool must be effective in ensuring that the level of protection guaranteed by the GDPR is not undermined by the transfer in practice.”

⁵¹¹ EDPB Recommendation 01/2020 (Version 2.0). Para. 29: “In particular, the protection afforded to the transferred personal data in the third country must be essentially equivalent to that guaranteed in the EEA by the GDPR, read in light of the Charter of fundamental rights of the EU.³⁹ This is not the case if the data importer is prevented from complying with its obligations under the chosen Article 46 GDPR transfer tool due to the third country’s legislation and practices applicable to the transfer, including during the transit of data from the exporter to the importer’s country.”

⁵¹² *Schrems II*. Para. 105.



Source: Rosenthal, D. [David], "EU SCC Transfer Impact Assessment Toolbox"⁵¹³

Clauses 14 and 15 of the third-countries-set provide evaluation criteria for the TIA such as the type of recipient, the categories and format of personal data transferred, the relevant laws and practices of the third country of destination, and contractual, technical, or organizational safeguards put in place to supplement the appropriate safeguards. Practical experience may also be included in the TIA. The footnote to clause 14 of the third-countries-set states:

As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third Parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular,

⁵¹³ Rosenthal, D. [David]. (2022). *EU SCC Transfer Impact Assessment (TIA) Toolbox*. https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx.

the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.⁵¹⁴

It is still disputed whether this formulation conceals a risk-based approach, as advocated by parts of the literature⁵¹⁵, or whether there is no room for such an approach due to a “0-tolerance” interpretation advocated by the EDPB⁵¹⁶ and NOYB⁵¹⁷. In this thesis, however, the risk-based approach will be followed, and therefore, as Diercks / Roth also summarized, “the principle of the risk-based approach of the GDPR must also be considered in a TIA within the meaning of Art. 46(2)(c) GDPR and clause 14 b) of the SCC and included via a proportionality assessment. Decisions of the EU Commission, such as the implementing decision on the SCC, are EU secondary law according to Art. 288 TFEU and are binding.”⁵¹⁸

On 10 November 2020, the EDPB issued its Recommendations 02/2020⁵¹⁹, which are intended to facilitate the TIA within “Step 3” of EDPB Recommendations 01/2020. The EDPB stipulated in Recommendation 02/2020 that it should be assessed whether the legislation in the third country meets the requirements of the “European Essential Guarantees”⁵²⁰. The EDPB also pointed out that the circumstances of the TFPD in question must be observed during the examination, because context-specific national regulations may exist in the third country.⁵²¹ The basis of this risk analysis should be the legal and actually “lived” level of data protection in the recipient country;⁵²² these circumstances are:

- Purposes for which the data are transferred and processed (e.g., marketing, HR, storage, IT support, clinical trials);
- Types of entities involved in the processing (public/private; controller/processor);
- Sector in which the transfer occurs (e.g., adtech, telecommunication, financial, etc.);
- Categories of personal data transferred (e.g., personal data relating to children may fall within the scope of specific legislation in the third country);
- Whether the data will be stored in the third country or whether there is only remote access to data stored within the EEA;
- Format of the data to be transferred (i.e., in plain text, pseudonymized or encrypted);
- Possibility that the data may be subject to onward transfers from the third country to another third country.

⁵¹⁴ Clause 14 of the third-countries-set.

⁵¹⁵ Diercks, N. [Nina] and Roth, M. [Markus]. (30 August 2021). *Data Transfer to unsafe Third Countries*. <https://www.wolterskluwer.com/en/expert-insights/data-transfer-to-unsafe-third-countries>.

⁵¹⁶ EDPB Recommendation 01/2020 (Version 2.0). P. 3.

⁵¹⁷ NOYB – European Center for Digital Rights. (2022). *noyb's comments on the proposed Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679*. https://noyb.eu/sites/default/files/2020-12/Feedback_SCCs_nonEU.pdf. P. 2.

⁵¹⁸ Diercks, N. [Nina] and Roth, M. [Markus]. (30 August 2021). *Data Transfer to unsafe Third Countries*. <https://www.wolterskluwer.com/en/expert-insights/data-transfer-to-unsafe-third-countries>.

⁵¹⁹ EDPB. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, (10 November 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

⁵²⁰ See also Chapter IX, Section III.3.

⁵²¹ EDPB. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, (10 November 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf. Para. 40.

⁵²² *Schrems II*. Para. 176

The TIA can therefore lead to two results:⁵²³

- The SDPC and / or BCR⁵²⁴, as appropriate safeguards in accordance with Art. 46 GDPR, ensure an adequate level of protection in relation to the specific circumstances of the processing and the legal situation in the third country. The transfer of personal data to third countries is then lawful.
- The legal situation in the third country prevents an adequate level of protection in relation to the specific circumstances of the processing, for example because the data importer cannot comply with the contractual obligations from the SDPC due to the laws in the third country that apply to him. In these cases, the transfer to third countries is only lawful if further steps (steps no. 4ff. below) are followed.

Step 4) Identification and implementation of supplementary measures

Data exporters are obliged to identify and implement measures that are suitable to provide for an essentially equivalent level of protection. In Annex 2 of EDPB Recommendations 01/2020 (Version 2.0), the EDPB lists possible measures based on use cases.⁵²⁵ A combination of different measures may be required. The EDPB points out that contractual or organizational measures alone will not be suitable for preventing access by public authorities in third countries and technical measures come into question. The EDPB proposes the inclusion of contractual rules, according to which the data importer for example names the laws applicable to him based on which access by public authorities to the personal data could take place; and in the absence of such laws, to provide the data exporter information and statistics on access by public authorities.

With the size of data records, the frequency of transfers, and a tendentially indefinite purpose of data usage, the risk that the data will become the subject of surveillance measures by the US authorities increases. A quantitative reduction in data volumes and data transmission processes, as well as clear purpose limitation, could mitigate that risk. Due to the US powers of intervention provided by EO 12333, transfers via the Internet are potentially more at risk than, for example, the dispatch of data carriers. The addressees of the data are also relevant: The criticized US surveillance programs primarily focus on large telecommunications companies; companies that send their data via cloud providers or external e-mail servers expose data to a greater risk, whereas corporate servers are likely to be less exposed. The type of backup and encryption of data should also be included in this assessment.

From a contractual perspective, the Parties involved in the data transfer could improve the level of protection by agreeing upon an obligation of the data importer to produce personal data only in the event of requests that are binding under the recipient country's applicable law. Voluntary cooperation of the data importer with the authorities to produce personal data would then infringe the contract on commissioned data processing. In addition to participating in the assessment of the legal framework in the recipient country, the data importer could also be submitted to further obligations to consistently inform the data exporter on the evaluation criteria. Therein, notifications about announced or completed requests by US authorities could be considered, although ex-post notification

⁵²³ EDPB. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, (10 November 2020),

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf. Para. 50.

⁵²⁴ The TIA must also be carried out for BCR. See EDPB. (23 July 2020). *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*. https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faoncjueuc31118_en.pdf. P. 3.

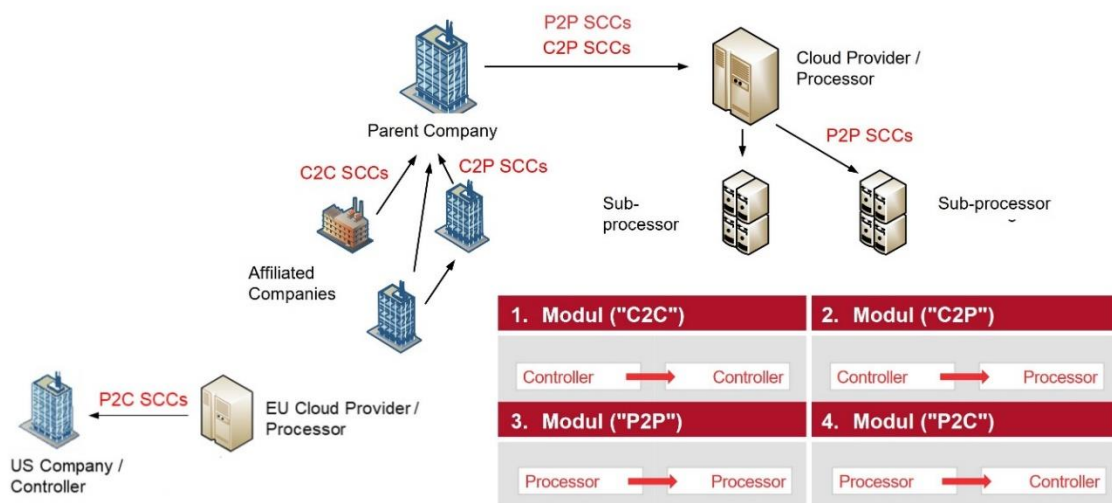
⁵²⁵ EDPB Recommendations 01/2020 (Version 2.0). Paras. 74 ff.

naturally does not protect against those that already had taken place. However, it could enable the data exporter to reassess future TFPD. A US data importer typically cannot assert any violations against data subjects in his own name due to a lack of standing. However, requests by US authorities should regularly also affect the rights of the data importers, which they could then assert in a claim before US courts in their own name. A supplementary measure could therefore be an obligation of the data importer to seek legal protection in US courts at the request of the data exporter and / or the data subjects concerned (third-party beneficiary effects). The data importer could contractually also be obliged to confirm that the software which the data importer uses does not contain any backdoors that would allow access by public authorities to personal data and that the importer is not obliged to provide the encryption key to those authorities. An obligation for physical transfer of data carriers could also be conceivable.

From an organizational perspective, data transfers taking place only within the EEA could solve the issue. If necessary, this could be achieved by changing group-internal access rights. Alternatively, data recipients in other third countries could also be considered for which an adequacy decision exists or for which the SDPC are less exposed to a weak level of protection. The conversion of all US data transfers to the legal basis of BCR to be approved by a SA could also be a solution as this could minimize the risk of a violation of the GDPR.

The third-countries-set will be examined more in detail below, as it has also extra-EU effect and thus falls more precisely in scope of the research objectives. The third-countries-set applies to transfers between a data exporter located in the EU/EEA and a data importer located outside the EU/EEA. This set combines general clauses with a modular approach to include various TFPD scenarios, according to the type of data exporter and data importer:

- Module 1: Controller-to-Controller Scenario ("C2C")
- Module 2: Controller-to-Processor Scenario ("C2P")
- Module 3: Processor-to-Processor Scenario ("P2P")
- Module 4: Processor-to-Controller Scenario ("P2C")



Source: BakerMcKenzie, "Standardizing data processing agreements globally"⁵²⁶

⁵²⁶ BakerMcKenzie. (3 August 2021). *Standardizing data processing agreements globally*, Webinar. https://f.datasrvr.com/fr1/321/63074/Standardizing_Data_Processing_Agreements_Globally.pdf. P. 8.

The general clauses in Sections I to III of the third-countries-set apply to all scenarios, whilst some clauses in Section II can differ in content depending on the scenario and corresponding Module.

Section I contains general provisions, e.g., on the scope and the contracting Parties, as well as references to GDPR definitions. The third-countries-set takes precedence over other contractual regulations (Section I Clause 4). Section I Clause 5 establishes, that in the event of a contradiction between the SDPC and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered thereafter, the SDPC shall prevail. Section I Clause 6 contains references to the appendices with a description of the data processing procedures and the technical-organizational measures. Section I Clause 7 opens the possibility of expanding the group of data exporters and importers to additional Parties, which then become part of the contractual provisions.

The core of the third-countries-set is Section II, which sets out obligations for the Parties, according to the applicable scenario. The duties of the data importer regulated in Clause 8 include provisions on transparency to hold the data subjects informed about the importers' identity/ies, storage limitations with confirmation of deletion by the importer, IT security and onward transfer. Clauses 9 to 11 contain further provisions on sub-processors, data subjects' rights and judicial redress. Clause 12 regulates the liability and exemption from penalties between the Parties. Clause 13 provides for information obligations of the data importer.

Clauses 2 and 3 of the third-countries-draft-set have been moved to Section III and are now Clauses 14 and 15 within the final version. They regulate the process of analyzing the legal framework in third countries. According to Clause 14, the Parties must carry out an assessment of the recipient country based on specific circumstances of the law in the third countries. The assessment must be documented and submitted to the SA upon request. Clause 15 defines the procedure with which the data importers must respond to requests from public authorities to disclose personal data. The importer must notify the exporter and data subjects about the request for disclosure and the circumstances of the individual case (15.1(a)). If notification to the exporter and / or data subjects is prohibited, the importer must try to act against the request for disclosure (15.1(b)). The importer must check the legality of such a request for disclosure on the basis of the local law prevailing and take all legally possible steps against this (15.2(a)), document the legal assessment and the procedure (15.2(b)) and ensure that a minimum of data are released (15.2(c)). The importer has to provide the exporter with regular reports with statistics on requests for disclosures (15.1(c)).

Section IV allows the data exporter to terminate the contract if the data importer does not comply with the legal obligations. Disputes must be settled by the courts of the EU Member States.

The third-countries-set has some positive key elements:

- The provisions are now more extensive and contain specific rules for several TFPD scenarios.⁵²⁷ This should make it easier for the data importers to assess their obligations and to uphold a level of protection that is essentially equivalent to the GDPR.

⁵²⁷ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Paras. 18, 31.

- The set addresses problems identified in *Schrems II* on third country's laws affecting compliance, access requests received by the data importer issued by third country's authorities and optional ad-hoc redress mechanism to the benefit of data subjects.⁵²⁸
- The set allows any entity to accede to the third-countries-set and to become a new Party to the contract as a controller or as a processor.⁵²⁹ This would avoid the need for a new data importer or new data exporter to join the previously concluded SDPC via a more complicated co-signing or signing on behalf.
- It has been clarified in Section I Clause 7 how the accession of new Parties to the third-countries-set must be given by the other Parties.⁵³⁰
- The Commission implemented to a significant extent the EDPB's recommendations. Clause 8.1 of Module 1 is no more divergent to the title of Clause 8.2 of Modules 2 and 3 which referred to "Purpose limitation". Several Clauses are now more consistent with the GDPR, particularly regarding data subjects' rights:

⁵²⁸ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Para. 19.

⁵²⁹ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Para. 45.

⁵³⁰ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Para. 46.

Clauses in third countries set	GDPR Arts.	Former divergence, which is now solved
Section II Module 1 Clause 8.2(a)	14(1), (2), (3)	List of information to be provided should be completed
Section II Module 1 Clause 1.5(a) and Section II Module 2 Clause 1.6 and Section II Module 3 Clause 1.6	Recital 26	Anonymized data does not open the applicability of the GDPR and should therefore not be included in the third countries set
Section II Module 1 Clause 1.5(a) and Section II Module 2 Clause 1.6 and Section II Module 3 Clause 1.6	4(12)	Definition of data breach
Section II Module 1 Clause 1.1 and Section II Module 2 Clause 1.2 and Section II Module 3 Clause 1.2	5(1)(b)	Aligning the wording
Section II Module 2 Clause 1.5 and Section II Module 3 Clause 1.6	28(3)(g)	Should be at the choice of the controller
Section II Module 2 Clause 1.9	28(3)(h)	Data importer cannot mandate audit. Bearing of the costs of the independent auditor is not regulated in the GDPR
Section II Module 1 Clause 5(a)	12(1), 15	Obligation imposed on the data importer to provide information to data subjects upon request
Section II Module 1 Clause 5(a)(i)	15(1)(d), 15(1)(e), 15(1)(g)	More information needed than those currently listed under Clause 5(b)(i), and more precisely
Section II Module 1 Clause 5(d)	22	Need to mirror GDPRs' prohibition of automated decision-making as a principle, and should set out the conditions allowing derogations to such prohibition
Section II Module 1 Clause 5(d)	15(1)(h), 22	Should require that information provided to data subjects include the significance and the envisaged consequences for data subjects

Improvable key elements of the third-countries-set are the following:

- The modular structure could lead to confusion about the area of application, since inside the respective clauses it is foreseen to choose from various TFPD scenarios.⁵³¹ The present structure unnecessarily increases the extent of the third-countries-set as such.
- There are some ambiguous, interpretable expressions: Section II Module 1 Clause 8.2(b), Section II Module 2 Clause 8.3 and Section II Module 3 Clause 8.3 use the expression “to the extent possible”. Protection provided by the third-countries-set should be fully ensured and without exceptions. Section II Module 2 Clause 8.5, Section II Module 3 Clause 8.5 and Section II Module 4 Clause 10 use the expression “local law”.

⁵³¹ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Para. 31.

This should be specified in more detail in a sense that only the requirements of local laws that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Art. 23(1) GDPR should be considered.

- There is still some a lack of consistency with the rules of the GDPR, which is outlined in the following table:

Clauses in third countries set	GDPR Arts.	Description of divergence
Section II Module 1 Clause 10(b)(iii)	17(1)	Should completely reflect the requirements set out in GDPR
Section II Module 1 Clause 10(c)	21	The right to object should not be limited to direct marketing cases
Section II Module 1 Clause 10(g)	12(4)	Information should be provided without delay and at the latest within one month of receipt of the request

- Section I Clause 3 should include a “positive list” of the rights that are enforceable by data subjects, instead of listing those that are not enforceable.⁵³² EDPB and the EDPS identified clauses which should be made enforceable by data subjects, including Section I Clause 3 itself.⁵³³
- It is not clear why Section III Clauses 14 and 15 apply to Module 4 only in certain cases. The Commission should further assess whether this exemption is justified.⁵³⁴ As the EDPB notes, it is also unclear if Clauses 14 and 15

cover situations where, in the absence of legislation in the third country affecting compliance with the commitments of the data importer, practices affecting such compliance would still have to be taken into account and assessed, or even if the clauses will cover practices diverging from what the legal framework of the third country provides.⁵³⁵ [...] These elements may give the impression that even when the prior assessment of the legal framework of the third country of the importer led to the conclusion that the legislation of the third country is not compliant with the EU requirements in terms of level of protection afforded to personal data and that no effective supplementary measure(s) could be put in place, transfers could still take place. The EDPB and the EDPS therefore recommend to clarify that these clauses will apply only to situations where, at the time of the conclusion of the contract, either the relevant law(s) of the third country was (were) assessed to be providing an essentially equivalent level of protection to that guaranteed within the EU, or where effective supplementary measures to remedy the potential deficiencies identified in such legislation and/or practices and to ensure the effective application of the safeguards contained in the Draft SCCs have been put in place so as to allow the data importer to comply with its obligations, or where the third country does not have any law in the field relevant to the transferred data.⁵³⁶

⁵³² EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Para. 33.

⁵³³ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Paras. 35-44.

⁵³⁴ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Para. 79.

⁵³⁵ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Para. 81.

⁵³⁶ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. Para. 84.

- Regarding Section II Clauses 11 and 13, it is unclear to which extent this mechanism would apply in relation to the specific and direct obligations of the processor and of the controller in Module 4.⁵³⁷
- It is unclear if Section II Module 8 is only relevant for independent or separate controllers, or if it could also be used in joint controllership scenarios with regard to processing of personal data carried out by joint controllers where one of the joint controllers is established outside of EEA/EU and thus not subject to the GDPR.⁵³⁸
- Section II Module 1 Clause 8.7 raises several issues. It does not include a commitment from the data importer to notify the data exporter of the existence of an onward transfer as it was the case in the 2004 SDPC for transfers from controllers to controllers.⁵³⁹ An obligation should be added for the Parties regarding the onward transfer(s) to assess whether the Parties are able to comply with the obligations set out by such agreement under the third country law applicable to this third Party, and, where necessary, to implement supplementary measures to ensure a level of protection essentially equivalent to the one required in the EEA.⁵⁴⁰ EDPB and EDPS also propose that an obligation should be added for the data importer to provide data subjects with a copy of the safeguards implemented for the onward transfer(s), upon request.⁵⁴¹
- Section II Module 2 Clause 8.8 should be completed with an obligation for the data importer to provide the data exporter, upon request, with a copy of the safeguards implemented for framing onward transfers to a third party. Such obligation was included in the controller to processor 2010 SDPC.
- The exact rationale of Section II Module 4 (Processor to Controller Scenario) is unclear. It allegedly includes only transfers from a processor subject to GDPR to its own controller not subject to GDPR, and excludes transfers from such a processor to any other controller.⁵⁴² It should be better determined which commitments shall be taken by Parties using Module 4⁵⁴³ and several obligations completed.⁵⁴⁴ Particularly, Module 4 Clause 10 would need clarification regarding the possible practical consequences entailed by the commitment made by the Parties to assist each other in handling data subjects' requests made on the basis of the data importer's applicable law.⁵⁴⁵

In November 2021, a discussion that had been going on for some time came to a head, which is why Moerel / van der Wolk even spoke of the assumption that "it is unlikely that

⁵³⁷ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Para. 114.

⁵³⁸ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Para. 47.

⁵³⁹ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Para. 53.

⁵⁴⁰ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Para. 55.

⁵⁴¹ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Para. 56.

⁵⁴² EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Article 1.1 and Recital 16.

⁵⁴³ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Para. 73.

⁵⁴⁴ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Paras. 74-78.

⁵⁴⁵ EDPB. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46scs_en.pdf. Para. 111.

the announced additional SCCs will materialize”⁵⁴⁶. This problem concerns the interaction between the application of Art. 3 GDPR and the provisions on international transfers under Chapter V of the GDPR. According to Recital 7 of the third-countries-set, a prerequisite for the application of this set is that the non-European data importer does not already fall within the territorial scope of the SDPC pursuant to Art. 3(2) GDPR.⁵⁴⁷ This announcement is a change in course for the Commission. This is because the previous SDPC did not contain any such restriction. Recital 7 leads to the possibility that the third-countries-set can no longer be used as supplementary measures in certain constellations. The background to the restriction may be that “transfer of personal data to a third country” has not yet been defined and thus an ambiguity about the scope of Chapter V of the GDPR has not yet been resolved. As *ratio legis* of Recital 7, it is conceivable that a data importer in a third country, whose activity falls within the territorial scope of the GDPR due to the nature of the data processing, does not need any contractually agreed supplementary measures. However, this contrasts with the assessment of the EDPB. The EDPB stated, that the transfer rules apply where factual transfers take place between the EU and non-EU countries, regardless of whether the non-EU data importer was already bound by GDPR.⁵⁴⁸ This is also the opinion of Kuner, who states that “as things now stand, Article 3 and Chapter V of the GDPR must be applied separately, and compliance with one does not remove the obligation to comply with the other when it is applicable”⁵⁴⁹. This is also followed by Moerel / van der Wolk when they justifiably said that “the position of the EDPB is further in line with the language of the GDPR, where Article 45 refers to transfers to countries that are considered not to provide an adequate level of protection. In other words, even if GDPR governs the relevant processing, the laws of the relevant country could prevent that despite the GDPR being applicable, an adequate level of protection could be ensured. In that sense, the SCCs do provide additional protection”⁵⁵⁰. Recital 7 of the third-countries-set therefore entailed an unclear legal situation. The Commission therefore published a FAQ document on SDPC and found that

the SCCs can therefore also be used by those non-EEA controllers and processors for data transfers related to these processing operations to non-EEA entities, in particular:

- By a controller outside the EEA whose processing is subject to the GDPR to a controller or processor outside the EEA that is not subject to the GDPR;
- By a processor outside the EEA whose processing is subject to the GDPR to a sub-processor or to a controller outside the EEA (on whose behalf it is processing the data) that is not subject to the GDPR.⁵⁵¹

The EDPB also published Guidelines 5/2021 on this legal issue:

Similarly, for a transfer of personal data to a controller in a third country less protection/safeguards are needed if such controller is already subject to the GDPR for the given processing. Therefore, when developing relevant transfer tools (which currently are only available in theory), i.e. standard contractual clauses or ad hoc

⁵⁴⁶ Moerel, L. [Lokke] and van der Wolk, A. [Alex]. (4 November 2021). *Why it is unlikely the announced supplemental SCCs will materialize*. <https://iapp.org/news/a/why-it-is-unlikely-the-announced-supplemental-sccs-will-materialize>.

⁵⁴⁷ “The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679.”

⁵⁴⁸ EDPB. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation*. (12 November 2019). Paras. 13 ff.

⁵⁴⁹ Kuner, C. [Christopher]. (2020). Art. 44. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 755–770). Oxford University Press. P. 758

⁵⁵⁰ Moerel, L. [Lokke] and van der Wolk, A. [Alex]. (4 November 2021). *Why it is unlikely the announced supplemental SCCs will materialize*. <https://iapp.org/news/a/why-it-is-unlikely-the-announced-supplemental-sccs-will-materialize>.

⁵⁵¹ European Commission. (25 May 2022). *Questions and Answers for the two sets of Standard Contractual Clauses*. https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf. P. 13.

contractual clauses, the Article 3(2) situation should be taken into account in order not to duplicate the GDPR obligations [...].⁵⁵²

In such a case, the deployed SDPC do not need to establish the protection of the GDPR, as the GDPR is already applicable under Art. 3(2) GDPR, but to protect against conflicting provisions of local law. However, SDPC tailored to this situation do not yet exist. The EDPB therefore proposed to the Commission: “The EDPB encourages and stands ready to cooperate in the development of a transfer tool, such as a new set of standard contractual clauses, in cases where the importer is subject to the GDPR for the given processing in accordance with Article 3(2).”⁵⁵³

The examination within step 4 can therefore lead to two results:

- The technical measures, together with the SDPC and / or BCR, and, if necessary, together with additional contractual and organizational measures, provide for an essentially equivalent level of protection.
- The supplementary measures do not provide such an essentially equivalent level of protection. In a realistic view to the legal landscape, this could currently apply to many data transfers to third countries, especially with the US.

Step 5) Procedural step

The procedural steps to be taken – if necessary, together with the SA – depend on the question which transfer tools under Art. 46 GDPR are used. SDPC, for example, may be supplemented (and included in a larger contract) if the supplement does not directly or indirectly contradict the SDPC. The alteration of rules entails that the responsible SA must approve the changed clauses, Art. 46(3)(a) GDPR.

Step 6) Regular evaluation

The principle of accountability requires the data exporter to continuously monitor the level of data protection in the third country and to identify developments that may impair the protection of the personal data transferred, Art. 5(2) GDPR. Sufficient mechanisms must be put in place to ensure that the data transfer can be suspended or terminated immediately if the data importer violates his obligations under the transfer tool used or if supplementary measures taken in the third country are no longer effective.

h. Art. 46(2)(d) GDPR (SDPC adopted by a SA and approved by the Commission as appropriate safeguard)

Art. 46(2)(d) GDPR provides for a division of labor between the Commission and national SAs in the development of such Clauses. This innovation opens a certain degree of flexibility for the SAs, with which they can take specific (national) data transfer matters into account if necessary. A SA can develop its content, the Commission examines it and approves it, Art. 93(2) GDPR. Once approved by the Commission, these SDPC can be used in all Member States. However, it remains to be seen to what extent the SAs will make use of this option in practice.

⁵⁵² EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021).

⁵⁵³ EDPB. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021). Para. 23.

i. Art. 46(2)(e) GDPR (CoC as appropriate safeguard)

Art. 46(2)(e) is intended to create incentives to establish CoC within the meaning of Art. 40 GDPR. An approved CoC requires legally binding and enforceable obligations on the part of the controller or the processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. In contrast to the BCR, approved CoC are usually not elaborated by individual groups but by entire industry associations and other associations that represent the interests of those responsible for the respective industry or service sector, which are then considered appropriate provided they have been approved by a SA and published by the EDPB. CoC are probably only tailored to data transfers between responsables that are bound by the same rules of conduct. CoCs are therefore intended for transfers "within" the group participating in the CoC. However, further information from the SAs on the scope of this tool remains to be seen.

j. Art. 46(2)(f) GDPR (certification mechanism as appropriate safeguard)

As part of a certification process in accordance with Art. 42 GDPR, companies can obtain certification from an accredited body in accordance with Art. 46(2)(f) GDPR to prove that data processing is in accordance with the law, also regarding data transfer to third countries. Reference should be made to the EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Arts. 42 and 43 GDPR⁵⁵⁴ as well as the EDPB Guidelines 4/2018 on the accreditation of certification bodies under Art. 43 GDPR⁵⁵⁵.

There are currently only a few accredited certification bodies in each Member State to issue these certificates; in Germany, e.g., there is only one⁵⁵⁶. Although the project of the certification provider AUDITOR⁵⁵⁷ was able to start in November 2017, it was already foreseeable at that time that a start of GDPR-based certification activities would hardly be possible in 2018, especially due to the lack of accreditation of certification scheme and certification bodies. The AUDITOR project, initially scheduled to run until October 2019, was extended to develop the standard based on the "Trusted Cloud Data Protection Profile" (TCDP) into a "European Data Protection Seal" in accordance with Article 42(5) second sentence GDPR. Another certification provider, Europrise⁵⁵⁸, after its certification scheme was recognized, still operates, like many other certification providers, on the accreditation of its certification criteria. This is mainly because within the European Framework, it is the national SAs that negotiate the criteria together with the EDPB. In Germany, as a federally structured country, there is even a third stakeholder involved in the elaboration of these criteria, the SAs of the federal States. In Germany, the criteria are not expected to be determined before the fall of 2023.

Certification mechanisms will have, in contrast to BCR or CoC, a specific area related to "IT-products" and "IT-services" in that they only cover certain processing methods, but not potentially all data processing activities by a controller or processor. Like CoC and BCR, approved certification mechanisms can at the same time also be recognized as appropriate guarantees for data transfers to third countries, provided that

⁵⁵⁴ EDPB. *Adopted Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, (4 June 2019).

⁵⁵⁵ EDPB. *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)*, (14 December 2018).

⁵⁵⁶ The "DAkKS" (*Deutsche Akkreditierungsstelle*) is the only national accreditation authority in Germany with European and international recognition.

⁵⁵⁷ <https://www.auditor-cert.de>.

⁵⁵⁸ <https://www.euprivacyseal.com>.

- the certification criteria have been approved by the competent SA or the EDPB, Art. 42(5);
- the respective data exporters and importers were, according to these criteria, accredited by the competent SA or the EDPB, Art. 42(5) GDPR;
- the certification criteria ensure appropriate guarantees for the protection of personal data. To this end, the certification criteria must also ensure compliance with the essential guarantees of European data protection law;
- the controllers and processors established in third countries have entered a legally binding and enforceable obligation to comply with the guarantees, including the rights of the data subjects, Art. 46(2)(f) GDPR.

While the competent SA can only certify based on the criteria approved by itself or by the EDPB, a certification body within the meaning of Art. 43 GDPR is not limited to this. According to Art. 43(2)(b) GDPR this certification body has beforehand to comply with the approved criteria according to Art. 42(5) GDPR.

k. Art. 46(3) GDPR (ad-hoc clauses approved by a SA as appropriate safeguards)

In addition to the safeguards listed in Art. 46(2) GDPR, which do not require the approval of a SA, Art. 46(3) and (4) provide for the possibility of TFPD to third countries or international organizations subject to approval by the competent SA. Art. 46(3) GDPR is non-exhaustive (“in particular”) and thus grants the flexibility necessary for practice. This flexibility considers the interest in a uniform application of the GDPR in the Union. The consistency procedure (Art. 46(4) GDPR) ensures that the requirements made by the individual SA for “appropriate safeguards” within the meaning of Art. 46(3) GDPR are essentially the same. In terms of content, appropriate safeguards, like all other types of appropriate safeguards within the meaning of Art. 46, must contain the essential data protection principles and essential guarantees of the GDPR. Art. 46(3) GDPR exemplarily lists two types of appropriate safeguards.

Art. 46(3)(a) GDPR refers to contractual clauses which do not correspond to the SDPC of Art. 46(2)(c) or (d) GDPR. Art. 46(3)(a) GDPR contracts are known as “ad-hoc clauses” between the Parties to the TFPD. They have the advantage that they can be applied in almost any constellation due to their customizability. Unlike the comparatively rigid SDPC, contractual clauses of Art. 46(3)(a) GDPR are adaptable to the respective purpose and location of use. An important innovation compared to Directive 95/46 is that a processor can also be considered as a data exporter, meaning that contractual clauses are generally also conceivable between a processor based in the EU and a sub-processor based in a third country. Under no circumstances, however, can “ad-hoc clauses” serve to lower the level of protection for the data subjects compared to the Commission’s SDPC. Such deviations from this level of protection would not only be classified as requiring a SA approval, rather they would not be approved according to Art. 46(3)(a) GDPR, thus the TFPD on such a basis would not be permitted at all.

According to Art. 46(3)(b) GDPR, provisions to be included into administrative arrangements between public authorities or bodies may also constitute appropriate safeguards for the TFPD. In contrast to Art. 46(2)(a) GDPR, this provision only covers administrative arrangements that are not legally binding. This can be assumed, for example, if the provisions are included in a “Memorandum of Understanding”.

I. Art. 49 GDPR (derogations for specific situations)

A transfer to a third country or an international organization could also be permitted under a derogation set by Art. 49 GDPR. Art. 44 GDPR requires all provisions in Chapter V of the GDPR to be applied to ensure that the level of protection guaranteed by the GDPR is not undermined, which implies that recourse to the derogations of Art. 49 GDPR should never lead to a situation where fundamental rights might be breached.⁵⁵⁹ As with the other permissions in Chapter V of the GDPR, Art. 49 does therefore not independently justify the transfer. We thus disagree with Neaf who found that

occasional data transfers using the contract-based derogation and the consent-based derogation in Article 49 GDPR may take place even if the third country of destination does not provide an adequate level of protection. However, these derogations both require some sort of agreement from the data subject for the transfer of their personal data and the data subject must be informed about the risks of the data transfers in question.⁵⁶⁰

We think that in addition to Art. 49 GDPR, the other provisions of the GDPR must also be considered. Nevertheless, the provision in Art. 49 seems to be suitable for such TFPD scenarios in view of the interpretation⁵⁶¹ of Art. 8 of the Charter, if such scenarios “do not allow for systematic, structural, and continuous data transfers”⁵⁶². Because then, Art. 49 GDPR “can be used to limit the right to continuous protection of personal data”⁵⁶³.

The CJEU maintained in *Schrems II* that TFPD based on Art. 49 GDPR remains possible.⁵⁶⁴ No legal “vacuum” can therefore arise because Art. 49 GDPR regulates that in the absence of an adequacy decision (Art. 45(3) GDPR) or of appropriate safeguards (Arts. 46 GDPR), a TFPD to a third country or an international organization can take place under certain conditions. During the period of legal uncertainty for US-based companies after *Schrems II*, “organizations may be inclined to look to the various derogations under Article 49 of the EU General Data Protection Regulation to see if these may provide alternative ways of transferring data. [...] There are specific recitals that relate to the derogations in Article 49, as well as detailed guidance from the EDPB.”⁵⁶⁵ Boyce / Hutt / Boardman have therefore done the work to examine Art. 49 GDPR for its possible applications in practice and have produced the following table⁵⁶⁶:

⁵⁵⁹ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 3.

⁵⁶⁰ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 424.

⁵⁶¹ See Chapter II, Section II.2.3.













⁵⁶² Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 424.







⁵⁶³ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 424.

⁵⁶⁴ *Schrems II*, Recital 202

⁵⁶⁵ Boyce, A. [Antonia] and Hutt, L. [Louise] and Boardman, R. [Ruth]. (May 2021). *Article 49 Derogations – Summary Table with Examples*. <https://iapp.org/resources/article/article-49-derogations-summary-table-with-examples>.

⁵⁶⁶ Red = Unlikely to be possible; Amber = May sometimes be possible; Green = Likely to be possible.

ARTICLE 49(1) DEROGATIONS	CONDITIONS FOR USE				EXAMPLES		
	Frequency — Does the transfer have to be “occasional” and “non repetitive”??	Necessity — Must the transfer be “necessary”??	Public authorities — Can the derogation be used by public authorities in exercise of their public powers? ⁶	Other requirements/ limitations/factors to consider	HR data	Business-to-consumer transaction	Clinical trials data
Consent — Article 49(1)(a)	N/A	No	No	High threshold to be met as consent must be explicit, ⁵ as well as “freely given, specific, informed” ⁶ and revocable ⁷ without detriment. ⁸			
Performance of contract between data subject and controller — Article 49(1)(b) OR performance of contract in interests of data subject between controller and another person — Article 49(1)(c)	Occasional only ¹⁰	Yes ¹¹	No	Necessity will be interpreted very narrowly and requires a “close and substantial connection” between the data transfer and the purposes of the contract. ¹²			
Important reasons of public interest — Article 49(1)(d)	N/A (but see “Other Requirements” column)	Yes ¹³	Yes	<ul style="list-style-type: none"> Can only be used for important public interests recognized under EU law or law of member state to which controller is subject.¹⁴ Although this derogation is not limited to occasional transfers only, transfers under this derogation should not take place “on a large scale and in a systematic manner,” or become “the rule” or in the usual course of business; they should be restricted to “specific situations.”¹⁵ Can be used by private entities, as well as public authorities. 			
Establishment, exercise or defence of legal claims — Article 49(1)(e)	Occasional only ¹⁶	Yes ¹⁷	Yes	<ul style="list-style-type: none"> Necessity test requires a “close and substantial connection” between the data and the specific establishment, exercise or defence of the legal position.¹⁸ Cannot be used to justify transfer on grounds of mere possibility that legal proceedings may be brought in future.¹⁹ 			

<p>Vital interests of the data subject or other persons — Article 49(1)(f)</p>	<p>Occasional or repetitive</p>	<p>Yes²⁰</p>	<p>Yes</p>	<ul style="list-style-type: none"> • Only applies where the data subject is physically or legally incapable of giving consent. • See Section 2.6 of the Article 49 Guidelines for further guidance on the narrow circumstances when this derogation may be used. 			
<p>Compelling legitimate interests — Article 49(1) sub-paragraph 2</p>	<p>Occasional only²¹</p>	<p>Yes²²</p>	<p>No</p>	<ul style="list-style-type: none"> • Can only be used for “residual” transfers²³ — this derogation is intended as a “last resort” where a transfer cannot be based on Article 45, 46, Article 49(1)(a)–(g) or Article 49 (1) sub-paragraph 2, and the data controller must be able to demonstrate this.²⁴ • Transfer must also only concern a limited number of data subjects.²⁵ • Controller must also assess all the circumstances of the transfer and, based on that assessment, provide “suitable safeguards,” inform supervisory authority of the transfer, and inform the data subject of the transfer and applicable “compelling legitimate interests.”²⁶ 			

Source: Boyce, A. [Antonia] and Hutt, L. [Louise] and Boardman, R. [Ruth], “Article 49 Derogations – Summary Table with Examples”⁵⁶⁷

The derogations in Art. 49(1) GDPR are to be interpreted strictly, so that the exception does not become the rule.⁵⁶⁸ It is still disputed how strict this interpretation must be. The EDPB noted that

the term occasional is used in Recital 111 [of the GDPR] and the term not repetitive is used in the compelling legitimate interests derogation under Article 49 par. 1 second sentence. These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals.⁵⁶⁹

The derogations of Art. 49(1) GDPR therefore seem generally not suitable for processings which are carried out massively, repeatedly, or routinely. In contrast, however, there are also opinions, such as by Moos / Flemming, that the “occasional” restriction intended by the EDPB is mentioned exclusively in the Recitals of the GDPR, but not in the normative text of Art. 49 GDPR, and therefore rejects the restrictive interpretation of the EDPB.⁵⁷⁰ Also complicating the interpretation of Art. 49(1) in this regard is the fact that, as the EDPB itself notes, “Recital 111 differentiates among the derogations by expressly stating that the “contract” and the “legal claims” derogations (Article 49 (1) subpar. 1 (b), (c) and (e)) shall be limited to “occasional” transfers, while such limitation is absent from the “explicit consent derogation”, the “important reasons of public interest derogation”, the “vital interests derogation” and the “register derogation” pursuant to Article 49 (1) subpar. 1 (a), (d), (f) and, respectively, (g)”⁵⁷¹. This indicates the intention of the GDPR to systematically decide between cases of the first sentence and those of the second sentence of Recital 111. If one were to interpret “occasional” strictly, many of the derogations of Art. 49(1) GDPR would not be applicable in practice,

⁵⁶⁷ Boyce, A. [Antonia] and Hutt, L. [Louise] and Boardman, R. [Ruth]. (May 2021). *Article 49 Derogations – Summary Table with Examples*.

https://iapp.org/media/pdf/resource_center/article_49_derogations_summary_table_with_examples_iapp.pdf.

⁵⁶⁸ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 4.

⁵⁶⁹ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 4.

⁵⁷⁰ Flemming, M. [Moos] and Rothkegel, T. [Tobias]. (2020). *EU-US-Datenschutzschild ungültig – Schrems II. Zeitschrift für Datenschutz*, 2020(10), 511–527. P. 527.

⁵⁷¹ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 4–5.

which would run counter to the CJEU, which wanted to avoid a “legal vacuum”. A more extensive interpretation is also supported by the fact that Art. 49(2) GDPR contains a new legal basis, not yet standardized in Directive 95/46, for a data transfer based on compelling legitimate interests of the controller, which, however, can only be used in exceptional circumstances under certain conditions; in this respect, “not repetitive” was probably inserted only in Art. 49(1) second sentence GDPR as a limiting manner, and “occasional” not to be understood as such limitation.

Art. 49(1)(a) permits a transfer to a third country or international organization if a data subject has expressly given its consent to the TFPD after being informed about the possible risks.⁵⁷² This information about risks is a specification of the requirements for the informed nature of the consent already required in Art. 4(11) GDPR. The data subject must be aware that its personal data may no longer enjoy the Union’s level of data protection after the TFPD. The information must contain the recipients in which countries the data are to be transferred to and if these countries belong to unsafe third countries, it must also be pointed out that the recipient country does not have a data protection level that is essentially equivalent to that of the Union. It must therefore be added in the information that the TFPD to an unsafe third country may result in specific risks, as the responsible for the TFPD have not provided safeguards to compensate for this deficit in protection. If specific risks are known, e.g. the lack of an independent SA or the possible access by public authorities, they must be pointed out.⁵⁷³ However, it cannot be required that data subjects must be made aware of all relevant details of the legal framework in the recipient country, which may come to light in the course of the TIA of the legal framework in the recipient country required by *Schrems II*, because this would probably lead to a too broad interpretation of the duty to inform.⁵⁷⁴ Art. 49(1)(a) GDPR does not provide any formal requirements for the consent. Alike for obtaining other consents, this means that, in addition to written consent, telephonic or oral consent is generally possible. The SAs apparently interpret the term “explicitly” to the extend that it only includes consent in the form of a declaration, in other words that a “clear affirmative action” fulfills the requirements for consent within the meaning of Art. 4(11) GDPR but not the requirements for consent within the meaning of Art. 49(1)(a) GDPR.⁵⁷⁵ The legislator therefore places higher requirements on consent to transfers to third countries. Fulfilling the requirements of Art. 49(1)(a) GDPR can be a challenge for those responsible for the transfer. There is a risk of ineffectiveness due to an incomplete or non-transparent information. Due to their business model, some responsible for data transfer might have no direct relationship with the data subjects and therefore could face practical hinderances to obtain consent. Difficulties can also arise from the requirement of a “freely given” consent. The consent of an employee could be somehow forced due to the contractual relationship between employer and employee.⁵⁷⁶ Furthermore, it could be a challenge for those responsible for the transfer to obtain and maintain the consent in a sufficiently “specific” manner, since technologies, business practices and the purposes of data processing are subject to constant changes and could trigger that consent forms need to be frequently changed. Consent can be revoked at any time, thus those responsible for the transfer might not want to rely on consent because of its lack of predictability. In addition, missing consent or its revocation could result in the need for those responsible for the transfer to technically split up the data records and partially

⁵⁷² Flemming, M. [Moos] and Rothkegel, T. [Tobias]. (2020). *EU-US-Datenschutzschild ungültig – Schrems II*. *Zeitschrift für Datenschutz*, 2020(10), 511–527. P. 527.

⁵⁷³ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 8.

⁵⁷⁴ Lange and Filip. (2020). DS-GVO Art. 49 Ausnahmen für bestimmte Fälle. In S. [Stefan] Brink and H. A. [Heinrich Amadeus] Wolff, *BeckOK Datenschutzrecht*. C.H. Beck. https://beck-online.beck.de/Bcid/Y-400-W-BECKOKDATENS-G-EWG_DSGVO-A-49-GI-A-II-1. Para. 8.

⁵⁷⁵ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 6.

⁵⁷⁶ See also the interpretation Art. 25(1)(a) Directive 95/46 in WP29. *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP114, (25 November 2005). P. 13.

refrain from such transfers. Apart from several scenarios limited purely to easy-to-handle online (on demand) services, consent as a mechanism is therefore still not much considered in practice.

Art. 49(1)(b) GDPR permits a TFPD to third countries if this TFPD “is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request”. Apparently, Meta changed the legal basis for such TFPD after *Schrems II* and declared the future use of SDPC as a transfer tool.⁵⁷⁷ Nevertheless, some argued already that Meta, alternatively, wants to justify the EU-US transfers on an alleged “necessity” of the transfer in accordance with Art. 49(1)(b) GDPR.⁵⁷⁸ However, the day when the GDPR became effective, Meta changed its privacy policy. Since then, Meta argued that users have a “contract” with the company and that no consent is required under data protection law. A more recent focus of discussion is the question of whether Meta has since then been processing its users’ personal data unlawfully, which resulted in the proceedings before the CJEU. The answer depends on whether Meta could reinterpret the consent given to send advertising into an existing contract with users to send advertising. If you create a profile on Facebook as a user, you have to accept the new terms of use including the “Privacy Policy”, the “Cookie Policy” and the “Legal Basis Information” since the GDPR came into force. This includes, for example, a declaration of consent by the user for the use of his data to provide personalized advertising. According to the terms of the contract, Facebook may also use sensitive data for this purpose. Facebook justifies this data processing by claiming that it is necessary to fulfill its contractual obligations. However, the Austrian Supreme Court did not consider this view to be self-evident at all.⁵⁷⁹ The key question is whether the user’s declaration of intent to process can be subsumed by the defendant under the legal concept of “performance of contract” so as to undermine the significantly higher protection that “consent” offers to the plaintiff. We too also of the opinion that the “necessity of data processing for the performance of a contract” depends on whether there is a direct factual connection between the intended data processing and the specific purpose of the legally binding relationship; we think that regarding Facebook this is not the case. Admittedly, the questions⁵⁸⁰ referred by the Austrian Supreme Court to the CJEU concern the “first stage”⁵⁸¹, i.e., the assessment of the lawfulness of the processing as such, and not directly to Art. 49 GDPR.

Art. 49(1)(b) GDPR also covers TFPD that are necessary to carry out pre-contractual measures. In these cases, the data subject is the contracting Party of the responsible, or the conclusion of a contract between these Parties is contemplated. In the case of pre-contractual measures, it must be prevented that possible contractual Parties take advantage of a still unclear situation for a TFPD to third countries. In addition, there must be a pre-contractual legal relationship based on started contract negotiations or a draft contract. In contrast to Art. 49(1)(b) GDPR, the data subject is not a contracting Party in the case of Art. 49(1)(c) GDPR, but a contract is concluded between controller and

⁵⁷⁷ Meta Inc. (17 August 2020). *Updating our international data transfer mechanisms*.

<https://www.facebook.com/business/news/updating-our-international-data-transfer-mechanisms>. // The Wall Street Journal, “Ireland to Order Facebook to Stop Sending User Data to U.S.”, 9 September 2020.

<https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980>.

⁵⁷⁸ NOYB, “Is the DPC actually stopping Facebook’s EU-US data transfers?! ..maybe half-way!”, 9 September 2020, <https://noyb.eu/en/dpc-actually-stopping-facebooks-eu-us-data-transfers-maybe-half-way>.

⁵⁷⁹ *Oberster Gerichtshof der Republik Österreich, OGH 6 Ob 56/2 1k*, ECLI:AT:OGH0002:2021:E132244, (23 June 2021).

⁵⁸⁰ 1) Whether Facebook can retroactively change one legal basis to another legal basis or exchange them; 2) whether personal data is processed excessively by Facebook combining and aggregating all collected datasets into one data pool; 3) whether Art. 9(1) GDPR can be interpreted to apply to the collection of certain categories of data; 4) whether a public statement on a sensitive category of personal data constitutes consent to ongoing data processing of that sensitive category of data

⁵⁸¹ See also Chapter II, Section II.3.4.4.a.

another natural or legal person different from the data subject. Centralization of personnel data management in a group of companies cannot be based on Art. 49(1)(b) GDPR, as it is not “necessary” for the individual employment relationship and it also exceeds the occasional character.⁵⁸² If an employment contract expressly refers to a matrix structure, e.g., of a MNE, and the associated obligations of the employee to work with staff in unsafe third countries, this could justify the “necessity” criterion of Art. 49(1)(b) GDPR.⁵⁸³ Art. 49(1)(b) GDPR is also applicable if TFPD are sufficiently regulated in the employment contract between the employee and the company, e.g., an employee’s responsibility for a major customer in an unsafe third country.⁵⁸⁴ Nevertheless, as NOYB correctly stated, Art. 49(1)(b) GDPR “may be an appropriate legal basis for very limited data transfers (e.g. when an EU user is sending an message to a US user), but cannot be used to outsource all data processing to the US”⁵⁸⁵.

A TFPD could also be permitted if it is necessary for the conclusion or performance of a contract concluded between the controller and another natural or legal person in the interest of the data subject, Art. 49(1)(c) GDPR. Art. 49(1)(a)–(c) GDPR do not apply to activities carried out by public authorities in the exercise of their sovereign powers, Art. 49(3) GDPR. To ensure the exceptional character of Art. 49 GDPR, this may only be understood as contracts that are clearly in the interests of the data subject, in particular so-called contracts in favor of third Parties; this contrasts with Art. 49(1)(b) GDPR where there is no such requirement. Art. 49(1)(c) GDPR does not apply, for example, where an organization has outsourced activities to SPs outside the EU/EEA for business purposes such as payroll management; although the data transfer to the SP serves to fulfill the service contract concluded between employer and employee, it has no significant added value for the employee.⁵⁸⁶

Art. 49(1)(d) and (e) GDPR could represent a derogation for cases of TFPD in investigative proceedings to US authorities and affiliated companies which are based in the US. This “pre-trial discovery” is a US civil procedural instrument that grants the Parties the right to inspect and transfer evidence such as documents held by the opposing party. Requests to produce personal data in these proceedings could conflict with the GDPR. In situations where there is an international agreement, such as a MLAT, EU companies “should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement”.⁵⁸⁷

Art. 49(1)(d) GDPR is consistent with the provision contained in Art. 26(1)(d) Directive 95/46, which is why interpretations below Directive 95/46 still apply to the GDPR.⁵⁸⁸ Arts. 49(4) and Art. 6(3) GDPR regulate that it must be a public interest that is recognized in Union law or in the law of the Member State to which those responsible for the TFPD are subject.⁵⁸⁹ Accordingly, aspects that are only in the interests of third countries cannot be considered. If, e.g., US authorities require to produce personal data for an investigation aimed at combatting terrorism, “the mere existence of EU or member state legislation also aimed at combatting terrorism is not as such a sufficient trigger to apply Article 49 (1)(d) GDPR”⁵⁹⁰. At this point, the difference to Art. 2(2)(d) GDPR has to be highlighted

⁵⁸² EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 8–9.

⁵⁸³ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 9.

⁵⁸⁴ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 9.

⁵⁸⁵ NOYB – European Center for Digital Rights. (9 September 2020). *Is the DPC actually stopping Facebook's EU-US data transfers?! ...maybe half-way!*. <https://noyb.eu/en/dpc-actually-stopping-facebooks-eu-us-data-transfers-maybe-half-way>.

⁵⁸⁶ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 12.

⁵⁸⁷ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 5.

⁵⁸⁸ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 10.

⁵⁸⁹ However, this was already the prevailing interpretation of Directive 95/46. See WP29. *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP114, (25 November 2005). P. 15.

⁵⁹⁰ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 10.

again: Art. 2(2)(d) GDPR excludes data processing of “competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security” from the scope of the GDPR. The scenario for “combating terrorism” addressed by the EDPB⁵⁹¹, however, concerns not an authority-to-authority transfer but a request from a public authority to a private entity to produce personal data. Art. 49(1)(d) only applies “when it can also be deduced from EU law or the law of the Member State to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation.” This “international cooperation” could be based on a bilateral agreement. If this agreement “recognizes a certain objective and provides for international cooperation to foster that objective, can be an indicator when assessing the existence of a public interest pursuant to Article 49(1)(d), as long as the EU or the Member States are a party to that agreement or convention”.⁵⁹² Public authorities as well as private entities, bound by this agreement, could then also rely upon Art. 49(1)(d) GDPR, because Recital 112 of the GDPR does not exclude private entities as examples; the EDPB also supports this interpretation by stating that “the essential requirement for the applicability of this derogation is the finding of an important public interest and not the nature of the organization (public, private or international organization) that transfers and/or receives the data.”⁵⁹³ Interestingly, the US Department of Commerce also took the position in its NTIA⁵⁹⁴ whitepaper, which is not legally binding, that after *Schrems II*, EU-US transfers can be based on Art. 49(1)(d) GDPR.⁵⁹⁵ From its point of view, the personal data accessed by US intelligence authorities may be evaluated by US authorities and passed on to the authorities of the EU Member States. EU authorities can then use these data to prevent attacks, prevent criminal offenses and ward off cyber-attacks. In this way, access to personal data under US law also serves the public interest of the EU – the processing could therefore be permitted under Art. 49(1)(d) GDPR. However, a restrictive interpretation of Art. 49(1)(d) GDPR is needed to prevent foreign authorities and courts from attempting to request the production of personal data from private bodies in the EU instead of using MLATs.⁵⁹⁶ It is unclear, however, whether priority should be given to MLATs over a direct request only in cases in which an international agreement (e.g., MLAT) exists with the requesting third country’s authorities and courts, or in general. According to the WP29, direct transfer by a private body to law enforcement or security authorities of a third country should only be permitted in particularly urgent cases (“questions of life and death”) and only if a direct transfer is provided for in the national law of the controller or in a MLAT.⁵⁹⁷ “Consequently, in a law enforcement context, it is very unlikely that such data processing can be legitimized on the basis of the consent of the data subject.”⁵⁹⁸

⁵⁹¹ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 10.

⁵⁹² EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 10.

⁵⁹³ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 11.

⁵⁹⁴ The NTIA is a division of the US Department of Commerce responsible for new technologies, among other things

⁵⁹⁵ Unites States Department of Commerce. (28 September 2020). *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*.

<https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>. P. 3.

⁵⁹⁶ WP29. *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP114, (25 November 2005). P. 15: “Any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in Directive 95/46.”

⁵⁹⁷ Article 29 Working Party. (28 November 2014). *Letter of 28 November 2014 to the Cybercrime Convention Committee*. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20141128_letter_of_the_art_29_wp_t-cy_on_the_cybercrime_scenarios_not_signed.pdf. P. 3.

⁵⁹⁸ Article 29 Working Party. (28 November 2014). *Letter of 28 November 2014 to the Cybercrime Convention Committee*. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20141128_letter_of_the_art_29_wp_t-cy_on_the_cybercrime_scenarios_not_signed.pdf. P. 5.

A public interest covers, for example, public health care (Art. 168, 191 TFEU), environmental protection (Art. 191 TFEU) and the public budget (Art. 126 TFEU). Compared to Art. 6(1)(e) GDPR, this derogation puts on a higher hurdle within the second stage test, since it is only for “important” reasons of the public. The GDPR makes no statement about when a reason of the public interest is to be regarded as “important”. With a view to the exceptional character, the GDPR must be interpreted restrictively.⁵⁹⁹

Processing of personal data, even if such important public interest applies, can in any case not take place “on a large scale and in a systematic manner; rather, the general principle needs to be respected according to which the derogations as set out in Article 49 shall not become “the rule” in practice but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test”.⁶⁰⁰

The scope of Art. 49(1)(d) GDPR is also restricted through Art. 2(2)(a) GDPR and Recital 16 of the GDPR, according to which the GDPR is not applicable to data processing in the context of activities that do not fall within the scope of Union law, such as activities in the area of a Members States’ national security.⁶⁰¹ Art. 49(1)(d) GDPR does neither apply to authority-to-authority transfers that fall within the scope of the LED.

Art. 49(1)(e) GDPR sets a derogation where the transfer is necessary for the establishment, exercise, or defense of legal claims. While Art. 49(1)(e) GDPR expressly requires a “legal claim”, it does not, however, apply to the transfer of informal official inquiries. Rather, it only covers inquiries that must have a basis in law, including a formal, legally defined process.⁶⁰² This procedure can be before courts or “responsible bodies”, and also includes activities carried out by public authorities in the exercise of their public powers, Art. 49(3) GDPR.⁶⁰³ Art. 49(1)(e) requires a close connection between the TFPD and a specific procedure in which the relevant data are necessary for the outcome of the procedure. The WP29 provided guidance to data controllers subject to EU Law in dealing with requests to TFPD to another jurisdiction for use in civil litigation and clarified when these transfers can be qualified as “necessary”.⁶⁰⁴ These interpretations of this previous provision in the Directive 95/46 still apply to Art. 49(1)(e) GDPR. Based on this guidance, the provision would only be a legal basis where such legitimate interests are not “overridden by the interests for fundamental rights and freedoms of the data subject”.⁶⁰⁵ The aims of an organization to act to promote or defend a legal right have therefore to be weighed against “the rights and freedoms of the data subject who has no direct involvement in the litigation process and whose involvement is by virtue of the fact that his personal data is held by one of the litigating Parties and is deemed relevant to the issues in hand, e.g. employees and customers”; this should “take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject”.⁶⁰⁶ The TFPD is not required if the procedure can be carried out with

⁵⁹⁹ WP29. *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP114, (25 November 2005). P. 7 & 14.

⁶⁰⁰ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 11.

⁶⁰¹ Recital 16 of the GDPR

⁶⁰² EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 11.

⁶⁰³ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018). P. 11.

⁶⁰⁴ WP29. *Working Document 01/2009 on pre-trial discovery for cross border civil litigation*, WP 158, (11 February 2009).

⁶⁰⁵ WP29. *Working Document 01/2009 on pre-trial discovery for cross border civil litigation*, WP 158, (11 February 2009). P. 9.

⁶⁰⁶ WP29. *Working Document 01/2009 on pre-trial discovery for cross border civil litigation*, WP 158, (11 February 2009). P. 9.

sufficient prospect of success without the data or, if possible, the transferred data can be restricted to anonymized or at least pseudonymized data.⁶⁰⁷

The TFPD may be permissible according to Art. 49(1)(f) GDPR, if it is “necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent”. Only the highest-ranking interests are relevant, in particular physical integrity and life.⁶⁰⁸ Examples are situations in which the data subject is in a life-threatening condition, and it is necessary for its rescue to transfer data of the person concerned to doctors in the third country. In the case of transfers to international humanitarian organizations for the fulfillment of tasks within the meaning of the Geneva Convention⁶⁰⁹ or for purposes of international humanitarian law in armed conflicts, there may be overlaps between Arts. 49(1)(e) and 49(1)(f) GDPR.

Art. 49(1)(g) GDPR regulates TFPD from registers which are intended to inform the public under Union law or the law of the Member States and are open to inspection either by the general public or by all persons who can demonstrate a legitimate interest, provided that the conditions for inspection specified in Union law or in the law of the Member States are met in the individual case. Unlike all other exceptions under Art. 49(1) GDPR, this derogation does not contain any restrictions on the purposes of the TFPD. However, transfers may not include all or entire categories of personal data contained in the register.

A transfer to a third country or to an international organization is permitted

if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer.⁶¹⁰

All requirements need to be met in a cumulative way, which means that the scope of its application is narrow. With the new derogation, the legislature opens up a certain degree of flexibility for cases in which there is an unavoidable need for a TFPD, but the TFPD can neither be based on Arts. 45 or 46 GDPR nor on one of the derogations in Art. 49(1) GDPR. To meet the protective purpose of Chapter V of the GDPR and the general principles of Art. 44 GDPR are not to be undermined by this catch-all element, the indefinite legal terms therein are all to be interpreted restrictively.

3.5. Law Enforcement Directive

The purpose of the LED is to

allow for smoother exchange of information between Member States’ police and judicial authorities. Criminal law enforcement authorities will no longer have to apply different sets of data protection rules according to the origin of the personal data. This will save

⁶⁰⁷ WP29. *Working Document 01/2009 on pre-trial discovery for cross border civil litigation*, WP 158, (11 February 2009). P. 10.

⁶⁰⁸ Recital 112 of the GDPR

⁶⁰⁹ International Committee of the Red Cross. *The Geneva Conventions and their Commentaries*, (1949), <https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions>.

⁶¹⁰ Art. 49(1) second sentence GDPR. This Article contains a new derogation that had no equivalent in the Directive 95/46.

time and money and increase the efficiency in the fight against crime. Having more harmonized laws in all EU Member States will make it easier for our police forces to work together.⁶¹¹

The LED applies to both the national and international processing of personal data (“processing” in the same sense as defined in the GDPR) by the competent authorities for the purposes of preventing, investigating, detecting or prosecuting criminal offenses or the execution of criminal penalties, including safeguards against and the prevention of threats to public security, Art. 1(1) LED. The LED does not apply to the processing of personal data during a processing activity which falls outside the scope of Union law or by Union institutions, bodies, offices and agencies, Art. 2(3) LED.

The requirements for lawful data processing laid down by the LED are largely known from the GDPR. Any processing of personal data requires a legal basis pursuant to Art. 8 LED, so that the LED, like the GDPR, is based on a so-called “prohibition principle” with certain derogations. In the absence of a consent, the LED does not imply any explicit requirements as to the prerequisites for effective consent. According to the Recitals of the LED, consent must be given in the same way as consent according to the GDPR.⁶¹² Art. 16 LED forces Member States to adopt provisions which entitle data subjects with the right to require the responsible authority to delete unlawfully processed or no longer required data and to correct data. However, to be able to exercise their rights under Art. 16 LED, data subjects must first know their personal which data are being processed. Arts. 12 and Art. 13 LED therefore provide that the controller shall inform the data subjects of the name and contact details of the controller, the purpose of the processing of the data and the existence of their rights. In addition to these notification obligations, the LED also specifies a right to information for data subjects in Art. 14 LED. Art. 13(3) LED allows the Member States to abolish, restrict or omit information obligations

to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to (a) avoid obstructing official or legal inquiries, investigations or procedures, (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, (c) protect public security, (d) protect national security, (e) protect the rights and freedoms of others.

According to the same criteria, the rights granted in Art. 15 LED can be restricted. Such derogations are necessary, particularly regarding covert investigations. These would lose their meaning if the investigation would have to be disclosed because of the right to information. However, the reasons for derogation are formulated in a vague manner. As a result, there is a risk that derogations may be utilized in several ways. Therefore, the question arises why the LED, as a specific regulatory instrument, does not explicitly distinguish between different investigations and provides for different consequences.

The LED covers data processing for both preventive and repressive purposes. A delimitation in Art. 2(2)(d) GDPR was therefore necessary because the GDPR would at

⁶¹¹ European Commission. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, Official Journal of the European Union, L 119/89, (4 May 2016). (“LED”). // European Commission. (14 April 2016). *Joint Statement on the final adoption of the new EU rules for personal data protection*. http://europa.eu/rapid/press-release_STATEMENT-16-1403_de.htm.

⁶¹² “In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities.” Recital 35 LED.

least partially apply to data processing covered by the LED. If a processing covered by the LED is carried out by an authority, the purpose of the processing determines whether the LED or GDPR apply. The GDPR does not apply to processing carried out in the exercise of activities that do not fall within the scope of European Union law, e.g., State security or national defense activities, and those carried out for the purposes of the LED.

Nevertheless, according to Recital 11 of the LED, the GDPR applies

in cases where a body or entity collects personal data for other purposes and further processes those personal data to comply with a legal obligation to which it is subject. For example, for the purposes of investigation, detection or prosecution of criminal offences, financial institutions retain certain personal data which are processed by them and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law.⁶¹³

Three TFPD scenarios are expressly listed in Recital 34 of the LED: First, “the rules of this Directive [LED] should apply to the transmission of personal data for the purposes of this Directive [LED] to a recipient not subject to this Directive”. Second, the GDPR should apply to the transfer if personal data covered by the LED is onwarded for other purposes. Third, if personal data processed for the purpose of the LED is further processed by the same authorities for other purposes, the GDPR should apply to the processings with that changed purpose. It is not clear from this Recital whether the lawfulness of the change of purpose is then governed by the LED or the GDPR.

Not all data processings for preventive purposes fall under the LED, but only if there is a certain connection to data processing for repressive purposes. How this relationship of closeness is to be understood has not yet been fully clarified. In Recital 12, the LED describes this relationship by giving examples from so-called “mixed constellations”: in the sense of a rule of doubt, an activity of an authority in a situation may also fall under the LED where it is initially not known whether a criminal offense has occurred.

3.6. Passenger Name Record and Advance Passenger Information Directives

The “Passenger Name Record Directive” (PNR Directive) was passed in a legislative package with the GDPR.⁶¹⁴ It had to be implemented by the Member States by 25 May 2018. The PNR Directive is different to the bilateral PNR agreements to be described below⁶¹⁵. The PNR Directive applies to the transfer of PNR data of flight passengers arriving from third countries to EU countries. Its scope has therefore extraterritorial reach beyond the Union. EU countries can decide to apply them to intra-EU flights. These data processing activities include collection, use and retention by Member States and exchange between Member States, Art. 2(1) PNR Directive. According to Art. 2(2)(d) GDPR, the processing of PNR data is excluded from the scope of the GDPR. Both PNR Directive and the LED follow the same protective scope as the GDPR and therefore comply with the EU’s consistency requirement. Recital 23 of the PNR Directive underscores that

⁶¹³ Recital 11 of the LED.

⁶¹⁴ European Commission. *Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Official Journal of the European Union, L 119/132 (4 May 2016). (“PNR Directive”).

⁶¹⁵ Chapter II, Section II.4.2.

the provisions of this Directive [PNR Directive] should be without prejudice to other Union instruments on the exchange of information between police and other law enforcement authorities and judicial authorities, including Council Decision of 6 April 2009 establishing the European Police Office (Europol)⁶¹⁶ and Council Framework Decision 2006/960/JHA⁶¹⁷. Such exchange of PNR data should be governed by the rules on police and judicial cooperation and should not undermine the high level of protection of privacy and of personal data required by the Charter, Convention 108 and the ECHR.

A Member State may transfer PNR data that are stored by the Passenger Information Unit (PIU) in accordance with Art. 12 PNR Directive to a third country on a case-by-case basis, if the conditions laid down in Art. 13 of 2008/977/JHA⁶¹⁸ are met, if the transfer is necessary for the purposes in Art. 1(2) PNR Directive, and the conditions of Art. 9(2) PNR Directive are met. The PNR Directive is limited to the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime, Art. 2(2) PNR Directive. The PNR Directive left considerable doubts as to its guarantees for fundamental rights. It provides for booking data of all travelers to the EU, from the EEA to third countries and, in some cases, also the data of travelers within the EU to be automatically forwarded to a police database and stored for up to five years. Critics such as Jan Philipp Albrecht, at that time spokesman for domestic and judicial policy for the Greens' European parliamentary group, therefore considered the first PNR Directive drafts' rejection of the EU Home Affairs Committee in 2013 and the referral back to the Commission as a great success for the rule of law and fundamental rights in Europe against data retention:

This EU PNR system is a false solution, based on the flawed political obsession with mass surveillance. PNR is a placebo at best, which will not only undermine the fundamental rights of EU citizens but also undermine the security of our societies by diverting badly-needed resources from security and intelligence tools that could actually be useful for combating terrorism, like targeted surveillance.⁶¹⁹

Parliament and Council agreed on a compromise text. Passenger data should be kept unmasked for six months and then stored for four and a half years without direct personal reference to “prevent, detect, investigate and prosecute” terrorist offenses and serious crime. In addition to intercontinental routes, intra-European routes are also to be recorded, the latter on a voluntary basis. For flights from and to the EU, up to 60 individual data points are collected. This includes address, seat number and flight number as well as meal requests, credit card data or IP addresses. The collection of PNR data concerns not only airlines, but also travel agencies or tour operators as well as other service providers, provided these make flight bookings. Information should be processed only from flights that start in or go to third countries. If Member States also apply the PNR Directive voluntarily to flights within the EU, then PNR data are scanned with relevant European databases, including the Schengen Information System (SIS II) or the Visa (VIS) database, as well as the Interpol database for stolen or missing travel documents. Further requests for disclosure can be made from Europol.

⁶¹⁶ Council of the EU. (15 May 2009). *Council Decision of 6 April 2009 establishing the European Police Office (Europol)*, 2009/371/JHA, OJ L 121, 37–66.

⁶¹⁷ Council of the EU. (29 December 2006). *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*, 2006/960/JHA, OJ L 386, 89–100.

⁶¹⁸ Council of the EU. (30 December 2008). *Council framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, 2008/977/JHA, OJ L 350/60. // Decision 2008/977/JHA of 27 November 2008 has been supplemented by the Law Enforcement Directive.

⁶¹⁹ The Greens/EFA. (14 April 2016). *PNR air passenger data retention*. <https://www.greens-efa.eu/en/article/pnr-air-passenger-data-retention-6837>.

On 24 July 2020, the Commission presented a report on the implementation of the measures set out in the PNR Directive.⁶²⁰ The Commission considered the collection and processing of PNR to be necessary and proportionate. In this regard, Member States reported that data transmitted in real time provided “tangible results in the fight against terrorism and crime”⁶²¹. According to the report, however, cooperation and exchange between PIUs is insufficient. The Commission attributed this to an unclear wording on spontaneous data transfers in the PNR Directive. The data quality is also improvable as the recording of the passenger’s date of birth by the airlines is not compulsory, which means that the incorrect spelling of the names can then not be detected by the PIU. The report also found shortcomings in the implementation of data protection requirements. Although these are “overall compliant”, some Member States have failed to adapt their national laws. It remained unclear which countries were involved as they were not mentioned in the report. The Commission did neither disclose the ways in which data protection provision were infringed. If, for example, the purpose limitation of data processing was to be circumvented to combat terrorism and serious crime, this would be a gross violation.

The EDPB sent on 22 January 2021 a letter to the Commission on the review of the PNR Directive.⁶²² Therein, it highlighted its support for the WP29 remarks, which found that the indiscriminate and long-term retention of PNR did not comply with the CJEU’s opinion on the envisaged PNR agreement with Canada.⁶²³ The EDPB also noted that the Commission’s report on the review of the PNR Directive does not provide sufficient information on the necessity and proportionality of collecting and processing PNR data indiscriminately, and requested the Commission to conduct a more detailed assessment to ensure compliance of all PNR instruments with CJEU case law.⁶²⁴ The EDPB argued that the review of the PNR Directive should be based on “solid and evidence-based elements able to demonstrate the connection between the PNR data retained and the objective pursued” and justified its opinion with the CJEU’s finding that “legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data retained and the objective pursued”.⁶²⁵ The EDPB also found that “the great amount of persons concerned compared to the little evidence for the usefulness of PNR data given in the few case studies up to now, raises serious doubts towards the proportionality of such mass data processing”.⁶²⁶

The Commission is to date opposed to amendment or expansion of the PNR Directive. Although in its Opinion 1/15⁶²⁷, the Court found the draft PNR Agreement between the

⁶²⁰ European Commission. *Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, SWD(2020)128 final, (24 July 2020).

⁶²¹ Nevertheless, the Commission did not publish the evidence sent by the Member States in this regard. See European Commission. *Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, SWD(2020)128 final, (24 July 2020) P. 7.

⁶²² EDPB. (22 January 2021). *Letter of 22 January 2021*, OUT2021-0004.
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letteronreviewpnrdirective.pdf.

⁶²³ EDPB. (22 January 2021). *Letter of 22 January 2021*, OUT2021-0004.
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letteronreviewpnrdirective.pdf. P. 1.

⁶²⁴ EDPB. (22 January 2021). *Letter of 22 January 2021*, OUT2021-0004.
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letteronreviewpnrdirective.pdf. P. 2 & 4.

⁶²⁵ CJEU. Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and others v Conseil des ministres*, Case C-511/18, ECLI:EU:C:2020:791. (“*La Quadrature du Net case*”). Para. 133.

⁶²⁶ 451.600 persons subject to further processing in one year (2018), 4.435.200 of them would have been sorted out and still, data of 1.016.400 persons would have been transmitted to competent authorities for further measures. See EDPB. (22 January 2021). *Letter of 22 January 2021*, OUT2021-0004.
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letteronreviewpnrdirective.pdf. P. 4.

⁶²⁷ CJEU. *Opinion 1/15 of the CJEU (Grand Chamber)*, ECLI:EU:C:2017:592, (26 July 2017).

EU and Canada⁶²⁸ to be incompatible with Articles 7, 8, 21 and 52(1) of the Charter, the CJEU appraised in *Ligue des droits humains* on 21 June 2022 for the second time the conformity of the PNR Directive with the Charter.⁶²⁹ It found that the PNR Directive was in line with the relevant parts of the Charter. The Court emphasized that the rules unquestionably represented a serious interference with, for example, the right to the protection of personal data. According to the CJEU, the powers under the PNR Directive must be interpreted narrowly. Then a TFPD in question could be considered limited to what is strictly necessary in the fight against terrorism and serious crime. This means that the system introduced by the PNR Directive may only extend to the information listed in the Annex to the PNR Directive. Moreover, the PNR system needs to be limited to terrorist offenses and serious crime with an objective connection to the transportation of passengers. In this regard, there would have to be a real and present or foreseeable terrorist threat to a Member State. Crimes that are mentioned in the PNR directive but fall under ordinary crime in the respective EU country should not be included. In addition, the extension of the PNR system to some or all EU flights must be limited to what is strictly necessary, the Court found.

The Court herewith “fixed” the PNR Directive through a Charter-compliant interpretation and, without affecting its validity, provided a set of interpretative limitations on the permissible scope and reach of EU-wide PNR security practices. Nevertheless, the CJEU left aside the two other EU legal instruments also considered in the judgment, namely the Advance Passenger Information Directive (API Directive)⁶³⁰ and Directive 2010/65/EU⁶³¹ on reporting formalities for ships. “European Digital Rights and Privacy International” (EDRi) commented on the CJEU’s judgment of 21 June 2022 that

on several key provisions, the Court grants a disproportionate degree of trust in the Member States to apply the PNR Directive in a restrictive way to meet the requirements of the Charter. For example, the Court counts on Member States to restrict the use of the PNR surveillance system in the fight against terrorism and serious crime, although the Directive does not adequately prevent risks of abuse by investigative authorities and the use of PNR data for ordinary crime.⁶³²

The main objectives of the API Directive are to combat irregular immigration and to improve border control. It regulates the collection and transmission of API data, which usually is contained in travel documents like passports and identity cards and collected by air carriers during check-in and transmitted by these carriers after check-in closure to the border control authorities of the country of destination. These authorities screen the passengers while in-flight for border migration management and law enforcement. The API Directive has extraterritorial effect, Arts. 2(b) and 3(1) API Directive. A data processing can also include “the purposes of allowing their use as evidence in proceedings aiming at the enforcement of the laws and regulations on entry and immigration”⁶³³. These processings must be carried out in accordance with their national

⁶²⁸ Which contains partly identical provisions to the PNR Directive.

⁶²⁹ CJEU. *Judgment of the Court (Grand Chamber) of 21 June 2022, Request for a preliminary ruling under Article 267 TFEU from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 17 October 2019, received at the Court on 31 October 2019, in the proceedings Ligue des droits humains v Conseil des ministres*, Case C-817/19, ECLI:EU:C:2009:68. (“*Ligue des droits humains*”).

⁶³⁰ Council of the EU. *Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data*, OJ L 261, 24–27, (6 August 2004).

⁶³¹ European Commission. *Directive of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC*, L 283/1, (10 October 2010).

⁶³² EDRi. (6 July 2022). *Mass surveillance of external travelers may go on, says EU’s highest court*. <https://edri.org/our-work/mass-surveillance-of-external-travellers-may-go-on-says-eus-highest-court/>.

⁶³³ Council of the EU. *Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data*, OJ L 261, 24–27, (6 August 2004), Recital 12.

law and subject to data protection provisions under Directive 95/46, Art. 6 API Directive. There were calls for an increased use of API data from international organizations to the participating States.⁶³⁴ In addition, since February 2018, the establishment of national API systems is an International Civil Aviation Organization (ICAO) standard. After enactment of the GDPR, there was therefore a need to revise the API Directive. The Commission underlined the “need to harmonize and clarify the way API data is collected throughout Europe; it also highlights the usefulness to combine API and PNR data in order to strengthen the reliability and effectiveness of PNR data as a law enforcement tool.”⁶³⁵ It therefore undertook a “Study on Advance Passenger Information (API) Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data”.⁶³⁶ Therein, it stated that “the API Directive does not point out to specific measures to safeguard data protection rights and only refers in general terms to Directive 95/46/EC. With the entry into force of the GDPR, the processing of personal data within the scope of the API Directive (for border control purposes) falls within its legal framework”. The Commission also found that the interplay between API Directive and PNR Directive seems to be unsure for the SAs in practice.⁶³⁷ Moreover, as the API Directive does not foresee any data retention requirements where API data are also used for law enforcement purposes, it has to be determined if the 24-hour limitation (Art. 6(1) API Directive) should also be applicable when processing API data for law enforcement purposes.⁶³⁸ The text of the API Directive “could benefit from a clearer reference to rights such as privacy, the protection of personal data and non-discrimination (respectively Articles 7, 8 and 21 of the Charter)”, especially to ensure that “none of the API data elements are based on a person’s race or ethnic origin, religion, political opinion, sexual life or sexual orientation”.⁶³⁹ In its Inception Impact Assessment, the Commission aimed to “repeal the API Directive and replace it with rules to ensure API data is processed evenly in the EU.”⁶⁴⁰ “The Commission saw the problem that

while the API Directive allows the use of API data for law enforcement purposes in accordance with national law, it does not specify conditions and safeguards for such processing. On the other hand, the PNR Directive includes provisions on the use of API data for law enforcement purposes. This partial overlap creates inconsistencies and uncertainty for both data subjects and national authorities on which data are collected and for which purpose.⁶⁴¹

The Commission therefore wanted to ensure effective processing of API data, while ensuring coherence with other EU instruments and facilitating legitimate travelers, combine API and PNR data to strengthen the reliability and effectiveness of PNR data

⁶³⁴ UN. UN Security Council, *Resolution 2178*, (2014). P. 5.

⁶³⁵ European Commission. (5 June 2020). *Border & law enforcement - advance passenger information (API) - revised rules*. https://ec.europa.eu/home-affairs/what-is-new/work-in-progress/initiatives/border-law-enforcement-advance-passenger-information-api-revised-rules_en.

⁶³⁶ European Commission. (February 2020). *Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data Final Report*. <https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF>. P. 50.

⁶³⁷ European Commission. (February 2020). *Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data Final Report*. <https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF>. P. 51.

⁶³⁸ European Commission. (February 2020). *Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data Final Report*. <https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF>. P. 51.

⁶³⁹ European Commission. (February 2020). *Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data Final Report*. <https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF>. P. 52.

⁶⁴⁰ European Commission. (5 June 2020). *Inception Impact Assessment*, Ref. Ares(2020)2916519. P. 2.

⁶⁴¹ European Commission. (5 June 2020). *Inception Impact Assessment*, Ref. Ares(2020)2916519. P. 2.

as a law enforcement tool, harmonize, facilitate access and use of API data for law enforcement purposes, and ensure appropriate data protection safeguards.

3.7. E-Evidence package

The complex EU legal framework in the area of criminal investigations affecting personal data consists of various Union instruments for cooperation in criminal matters, such as “Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the “European Investigation Order in criminal matters” (EIO Directive)⁶⁴², the “Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union”⁶⁴³, the “Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime”⁶⁴⁴, the “Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation” (Europol)⁶⁴⁵, the “Council Framework Decision of 13 June 2002 on joint investigation teams”⁶⁴⁶, and bilateral agreements between the Union and third countries, such as the EU-US MLAT⁶⁴⁷ and the EU-Japan MLAT⁶⁴⁸.

The Commission announced a legislative proposal to “strengthen the Europol mandate in order to reinforce operational police cooperation”⁶⁴⁹. The Council had noted before “that Europol could fulfil its role more effectively if it were able to “gather and process data available in the online environment, including data requested and obtained directly from private Parties, notwithstanding Europol’s obligation to notify the relevant national competent authorities of the Member States as soon as these are identified”⁶⁵⁰. In its Inception Impact Assessment of 14 May 2020, the Council outlined the objective “to streamline Europol cooperation with third countries.”⁶⁵¹ On 4 May 2022, the Parliament strengthened the mandate of Europol to collect personal data, including data from countries outside the Union, and introduced measures for data protection, including the appointment of a fundamental rights officer at Europol and independent oversight by the EDPS.⁶⁵² This draft “effectively overturns an order by the European Data Protection

⁶⁴² European Commission. *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters*, OJ L 130, 1–36, (1 May 2014). (“EIO Directive”).

⁶⁴³ Council of the EU. *Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, OJ C 197, 1–2, (12 July 2000).

⁶⁴⁴ Council of the EU. (6 March 2002). *2002/187/JHA: Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime*, OJ L 63, 1–13.

⁶⁴⁵ European Commission. *Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA*, OJ L 135, 53–114, (24 May 2016).

⁶⁴⁶ Council of the EU. (20 June 2002). *Council Framework Decision of 13 June 2002 on joint investigation teams*, OJ L 162, 1–3.

⁶⁴⁷ EU. *Agreement on mutual legal assistance between the European Union and the United States of America*, OJ L 181, 34–40, (19 July 2003). (“EU-US MLAT”).

⁶⁴⁸ EU. *Agreement between the European Union and Japan on mutual legal assistance in criminal matters*. OJ L 39, 20–35, (12 February 2010). (“EU-Japan MLAT”).

⁶⁴⁹ European Commission. (2020). *Police cooperation – stronger mandate for Europol*. Ref. Ares(2020)2555219.

<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate>.

⁶⁵⁰ Council of the EU. (2 December 2019). *Council conclusions on Europol’s cooperation with Private Parties*, 14745/19, ENFOPOL 526. P. 2.

⁶⁵¹ European Commission. *Commission Staff Working Document, Impact Assessment, Accompanying the document Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol’s cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol’s role on research and innovation*, SWD/2020/543 final, (9 December 2020). P. 14.

⁶⁵² European Parliament. (4 May 2022). *Parliament backs giving more powers to Europol, but with supervision*. <https://www.europarl.europa.eu/news/en/press-room/20220429IPR28234/parliament-backs-giving-more-powers-to-europol-but-with-supervision>.

Supervisor (EDPS) in January 2020 that required Europol to delete swathes of personal data it had collected and processed unlawfully”⁶⁵³.

A law enforcement authority that wanted to access data stored in another Member State during its investigations so far had to contact the authorities of the Member State in which the data was stored. The answer to this request depended on the law of the Member State on whose territory the servers were located. The procedures for this were based on the MLAT applicable to this case. The Commission assumed that MLATs are too slow and cumbersome and cannot be reformed in a way it would make them faster and more effective and was therefore striving for new regulation.⁶⁵⁴ Its initiative was also motivated by the significant legal challenges that the globalization of criminal evidence was creating for law enforcement authorities.

The year 2018 was marked by some important legislative initiatives in the US and the Union reflecting a new approach concerning law enforcement access to electronic evidence. On 17 April 2018, the Commission presented a so-called “E-Evidence package”, consisting of a “Proposal on European Production and Preservation Orders for electronic evidence in criminal matters” (E-Evidence Regulation) and a supplementing “Proposal for a Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings” (E-Evidence Directive).⁶⁵⁵

For reasons of legal certainty, new regulatory instruments had become necessary, as “cross-border request to obtain e-evidence is made in over 50% of all criminal investigations”⁶⁵⁶. The E-Evidence package is “intended to bring clarity and legal certainty, and they should considerably speed up the process of obtaining e-evidence, with an obligation for SPs to respond within 10 days and up to 6 hours in cases of emergency (compared to an average of 10 months within the Mutual Legal Assistance procedures)”⁶⁵⁷. The rules of the E-Evidence-Regulation “will create a European Production Order, create a European Preservation Order, include strong safeguards, oblige service providers to designate a legal representative in the Union and provide legal certainty for businesses and service providers”⁶⁵⁸, reported the Commission in 2019.

The E-Evidence Regulation does not replace the EIO Directive but provides authorities with an additional tool, as there might be situations where the EIO Directive could be the

⁶⁵³ Computer Weekly. (16 May 2022). *Europol gears up to collect big data on European citizens after MEPs vote to expand policing power*. <https://www.computerweekly.com/news/252518218/Europol-gears-up-to-collect-big-data-on-European-citizens-after-MEPs-vote-to-expand-policing-power>.

⁶⁵⁴ EU Justice Commissioner Věra Jourová said that “we have to find ways that investigative authorities can access data outside the EU if the MLAT channel is not adequate or available”. See European Commission. (25 April 2016). *EU Criminal Law – key to a Security Union based on fundamental rights and values*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_16_1582.

⁶⁵⁵ European Commission, *Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, COM/2018/226 final - 2018/0107 (COD), (17 April 2018). (“E-Evidence Directive”).

⁶⁵⁶ Council of the EU. (15 February 2023). *Better access to e-evidence to fight crime*. <https://www.consilium.europa.eu/en/policies/e-evidence>. // European Commission. *Commission Staff Working Document, Impact Assessment, Accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118 final, (17 April 2018). P. 14.

⁶⁵⁷ European Commission. (2018). *Improving cross-border access to electronic evidence in criminal matters*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1453-Improving-cross-border-access-to-electronic-evidence-in-criminal-matters_en.

⁶⁵⁸ European Commission. (2019). *E-evidence - cross-border access to electronic evidence*. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

preferred option for the authorities. The Commission announced that creating a new electronic evidence tool is a better alternative than amending the EIO Directive, as the collection of electronic evidence presents certain challenges that investigative measures of the EIO Directive do not cover.⁶⁵⁹

The E-Evidence Regulation is to be distinguished from the bilateral proceedings between the Commission and the US to negotiate international agreements on e-evidence in criminal matters and is

limited to requests for stored data (data from real-time interception of telecommunications is not covered) and to orders issued in criminal proceedings for a specific criminal offence under investigation. It therefore does not cover crime prevention or other types of proceedings or infringements (such as administrative proceedings for infringements of the rules of law) and does not require providers to systematically collect or store more data than they do for business reasons or for compliance with other legal requirements.⁶⁶⁰

A European Production Order or a European Preservation Order can therefore only be issued in the context of criminal investigations or criminal proceedings for specific criminal offenses. This distinguishes them from preventive measures or legally stipulated obligations for data retention. The relevance of this “data subject categorization” was also indicated by an order of the EDPS to Europol, demanding “to delete data concerning individuals with no established link to a criminal activity”⁶⁶¹.

In spring 2018, the US Congress passed the Cloud Act, which allows US investigative authorities to access data stored on foreign servers. This Act resolved the *Microsoft Ireland* case⁶⁶² which was then declared closed. The Cloud Act enabled US authorities to access e-evidence that is processed outside of the US.

The E-Evidence Regulation version of 17 April 2018 was similarly designed to give authorities in Europe access to evidence online. According to Art. 2(3) of this version, those responsible for the data processing are natural or legal persons which provide electronic communication services or information society services, including social networks, online marketplaces, and other hosting services. The term “information society service” has the same meaning as in Art. 8(1) GDPR. According to Art. 2(6) of this version, “electronic evidence” means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data”. These data types are described in more detail in Art. 2(7)–(10) of this version: This data includes above all the customer’s identity and address data, transactional data, as well as content data such as all data stored in a digital format (such as text, voice, videos, images and sound recordings). This means that the term “electronic evidence” basically includes all essential data that a company holds about a user. The only exception is real-

⁶⁵⁹ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 3.

⁶⁶⁰ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 6.

⁶⁶¹ EDPS. *EDPS orders Europol to erase data concerning individuals with no established link to a criminal activity*. https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en, (10 January 2022).

⁶⁶² See also below Chapter III, Section II.1.2.7.

time data.⁶⁶³ Art. 5(4) of this version provides that access to transactional and content data should only be possible in restricted scenarios, for example in the case of crimes for which there is a minimum penalty of 3 years. The personal data covered by this version may only be processed in accordance with the GDPR and the LED.⁶⁶⁴

Arts. 3(1), 2(4), and the Recitals of this version result in extraterritorial effects, as the provisions can also apply to providers outside the Union, which direct their services to Member States citizens, or which use legal or natural persons inside the Union for enabling their services.⁶⁶⁵ The reasoning of this extraterritorial application was described as follows, which highlighted the alignment with the GDPR:

The active offering of services in the Union, with all the benefits deriving from it, justifies that these service providers are also made subject to the regulation and creates a level playing field between participants on the same markets. Moreover, not covering these service providers would create a gap and make it easy for criminals to circumvent the scope of the regulation.⁶⁶⁶

However, the mere accessibility of a service should not be a sufficient prerequisite for the application of the E-Evidence Regulation, since accessibility of, e.g., a website of the SP or his agent would then lead to a potentially global reach of the E-Evidence Regulation. Therefore – alike the statements of the CJEU in the *Google Spain* judgment – a significant connection between the provider and the territory in which it offers his services is necessary. Such connection exists where a SP has an establishment in one or more Member States or due to the existence of a significant number of users in one or more Member States or the focus of activities on one or more Member States.⁶⁶⁷ The focus of activities on one or more Member States can be determined “on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in a Member State”⁶⁶⁸. These factors could include the availability of an app in the respective app store for a certain national territory, the placement of local advertisements or advertising in the language used in a Member State, or the use of information by people in the Member States in the course of activities or from the management of customer relationships. As an additional requirement, the requested data must be related to the services of the provider in the Union.

⁶⁶³ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 6: “data from real-time interception of telecommunications is not covered”.

⁶⁶⁴ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 3.

⁶⁶⁵ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 6: “The service provider running the infrastructure are under a different national legal framework, within the Union or beyond”. // European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 13: “Moreover, the Regulation is also applicable if the service providers are not established or represented in the Union, but offer services in the Union.”

⁶⁶⁶ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 15.

⁶⁶⁷ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 15.

⁶⁶⁸ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 15. // The proposal also refers to Article 17 (1) (c) of the so-called Brussels 1a Regulation (No 1215/2012), which defines the jurisdiction for matters relating to a contract concluded by a person, the consumer, for a purpose which can be regarded as being outside his trade or profession

Arts. 15 and 16 of this version dealt with a “European Production Order Certificate” (EPOC) and a “European Preservation Order Certificate” (EPOC-PR) to addressees in third countries and provide for a procedure in case of conflicting obligations deriving from the law of a third country. The Union apparently learned from the drawbacks of the Cloud Act, which in the public opinion threatened the protection of fundamental rights. This version of the E-Evidence Regulation wanted to solve this by including “strong safeguards and explicit references to the conditions and safeguards already inherent in the EU acquis, thus serving as a model for foreign legislation”; this version was intended to set a high level of protection to motivate third countries to provide a similarly high level of protection.⁶⁶⁹ The Union also wanted to revive transatlantic diplomatic conventions with this procedure. In a case in which authorities from third countries request a Union citizen’s personal data to be produced by an EU-based SP, the legal provisions of the Union or of the Member States for the protection of fundamental rights could prevent disclosure. The Union expected third countries to respect such prohibitions for their part, so a reciprocity. This version therefore set out a specific “conflicts of obligations” clause that allows SPs to identify and raise conflicting obligations they may face; the procedure triggers a judicial review.⁶⁷⁰ This procedure can be started by the addressee of a European Production Order, if compliance with a European Production Order would cause a breach of the law of a third country that prohibits the disclosure of data on the grounds of a necessity to protect either the fundamental rights of the data subjects or the fundamental interests of the third country in connection with national security or defense. The addressee is then obliged to inform the issuing authority by means of a reasoned objection of the grounds for its conclusion of facing contradicting obligations. The objection cannot be based solely on the fact that there are no comparable provisions in the law of the third country, nor on the fact that the data are stored in a third country. The objection is to be raised according to the procedure of Art. 9(5) of this version of the E-Evidence Regulation for the notification of an intended non-compliance, using the form in Annex III. Since the European Preservation Order itself does not lead to the disclosure of data and therefore does not cause comparable concerns, the aforementioned procedure was limited to the European Production Order.

Based on the grounds for this objection, the issuing authority then reviews its own order. If the issuing authority decides to withdraw the order, the procedure is ended. If the issuing authority wishes to uphold the order, the case is forwarded to the competent court in its Member State. Considering all facts relevant to the case, the court then examines whether the legal provisions of the third country apply in the present case and, if they do so, whether there is actually a conflict. The court hereby considers whether the third country’s law is not aimed at protecting fundamental rights or interests of the third country in relation to national security or defense, but is more obviously aimed at protecting other interests, or used to protect unlawful acts from requests by law enforcement agencies in the context of criminal investigations. If the court concludes that there is indeed a conflict with obligations arising from legal provisions protecting the fundamental rights of individuals or fundamental interests of the third country in connection with national security or defense, the court must address the national central authorities of the third country concerned and request an opinion from the third country. If the third country consulted confirms the existence of the conflict and objects to the execution of the order, the court must withdraw the order. If the conflict arises based on other third country law that does not serve either to protect the fundamental rights of individuals or the

⁶⁶⁹ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 21.

⁶⁷⁰ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 21 f.

fundamental interests of the third state in connection with national security or defense, the Member State court shall rule by its own balancing of interests in the case. The obligations set out in Art. 9 of this version also apply if the law of a third country results in obligations that contradict one another. If the court concludes that the order is to be upheld, the issuing authority and the SP are informed that the order can begin to be executed. If the order is suspended, a separate European Preservation Order can still be obtained based on a MLAT.

The procedure under Art. 15 of this version of the E-Evidence Regulation was created to ensure compliance with two types of laws: on the one hand, with so-called “blocking statutes”⁶⁷¹, which prohibit, e.g., disclosure of content data within its geographical scope except under certain conditions; and on the other hand, with laws that prohibit disclosure not generally, but in individual cases. The E-Evidence Regulation could also improve transborder access to electronic documents in criminal investigations and save investigators bureaucratic coordination across national borders, which would open an alternative path to MLATs.⁶⁷² If there is infrastructure used in which the electronic evidence is stored and the service provider that operates the infrastructure within or outside the Union falls under a different national legal framework than the victim or the offender, it can be time-consuming and difficult for the issuing State to gain access to electronic evidence across borders without harmonized minimum requirements. Member States acting alone on basis of non-harmonized rules could lead to fragmentation of legal frameworks in Member States, which was identified as a major challenge by SPs seeking to comply with requests based on different national laws.⁶⁷³ It therefore cannot be denied that the design of this version of the E-Evidence Regulation had a legitimate purpose. In fact, immediate access to data stored in a cloud service is becoming more and more important to guarantee effective and fair criminal justice in an increasingly digitized reality.

The main advantage of this version of the E-Evidence Regulation was to allow for direct cooperation with SPs, regardless of their Member State of establishment or the location of the data. But there were also downsides of the E-Evidence Regulation:

Given its binding effect for Member States, the E-Evidence Regulation could have a considerable impact on fundamental rights of EU citizens.⁶⁷⁴ A study by “European Parliament’s Committee on Civil Liberties, Justice and Home Affairs” (LIBE)⁶⁷⁵ stated that this version “suffers from major shortcomings”⁶⁷⁶. Former German Federal Data Protection Commissioner Peter Schaar expressed that a TFPD for the purpose of criminal investigation is favorable, however it should not be at the expense of the rule of

⁶⁷¹ See also below Chapter VIII, Section III.

⁶⁷² According to the Commission, it takes an average of ten months for a request for legal assistance to be successful. See European Commission. (5 February 2019). *Security Union: Commission recommends negotiating international rules for obtaining electronic evidence*. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_843.

⁶⁷³ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 6.

⁶⁷⁴ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). P. 9–10.

⁶⁷⁵ LIBE “is in charge of most of the legislation and democratic oversight for policies enabling the European Union to offer its citizens an area of freedom, security and justice (Article 3 TEU) [...] and while doing so it ensures the full respect of the Charter of fundamental rights in the EU territory in conjunction with the European Convention on Human Rights and the strengthening of European citizenship”. See European Parliament. (2023). *About LIBE*. <https://www.europarl.europa.eu/committees/en/libe/about>.

⁶⁷⁶ European Parliament. *An assessment of the Commission’s proposals on electronic evidence*, PE 604.989, (September 2018), [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU\(2018\)604989_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf). P. 6–7.

law, in particular legal protection.⁶⁷⁷ He warned of “instruments that are sometimes questionable under the rule of law. [...] Authorities from countries like Romania or Hungary, for which the EU has expressed strong doubts about their rule of law for a good reason, would have direct access to data that providers have collected in other Member States⁶⁷⁸”, said Schaar. He also raised the problem that a review by a domestic court or a judicial authority is not intended, which would mean that data would also have to be transmitted to foreign bodies for which domestic authorities do not have a corresponding authorization. He further found that criminal procedural safeguards are circumvented if the law of the issuing State does not provide for such. The EDPS expressed its concern “that the important responsibility of reviewing compliance of EPOC and EPOC-PR with the Charter is entrusted to SPs. The EDPS recommended “involving judicial authorities designated by the enforcing Member State as early as possible in the process of gathering electronic evidence”⁶⁷⁹. Burchard raised the concern that specific requirements for the suspicion, for the allegation of evidence (that data are stored by a SP) and the scope of evidence (to what extent these data may be queried) are not found in this version, so that it *de facto* promotes large-scale “fishing expeditions”⁶⁸⁰. He also criticized that no distinction is made between different cloud models.⁶⁸¹ Users who store their data “free of charge” with SPs are treated equal as users who pay for a good protection of their personal data. This does not consider the fact that cloud data are not always volatile. On the contrary, certain cloud models are based on a data being stored “securely” in certain locations. In substance, this version therefore treated unequal in the same way (different cloud models and user behavior). He furthermore found that this version also curtailed the legitimate business interests of those SPs which are justifiably increasingly rewarded for their customers’ trust in the security of their personal data. In addition, this version treated access to subscriber and transactional data as less intrusive than access to content data, which is no longer appropriate in the context of Big Data for example, because precise, highly invasive movement profiles can be created from the accumulation of access data.⁶⁸² Associations such as the “Chaos Computer Club”⁶⁸³ and EDRi also listed their concerns in an open letter.⁶⁸⁴ They resumed that this version weakens the ability of authorities [in other countries] to oppose enforcement of an order based on a violation of the Charter, incorrectly assumes that non-content data are less sensitive than content data, brings into play the possibility of making orders without a court order, brings no legal certainty [for those affected], and undermines the role of the enforcing states, and thus judicial cooperation.

⁶⁷⁷ Peteranderl, S. [Sonja]. (11 June 2019). Alle Daten an alle Staaten. *Der Spiegel*. <https://www.spiegel.de/netzwelt/netzpolitik/e-evidence-warum-die-eu-plaene-zu-digitalen-beweisen-gefaehrlich-sind-a-1270939.html>.

⁶⁷⁸ Peteranderl, S. [Sonja]. (11 June 2019). Alle Daten an alle Staaten. *Der Spiegel*. <https://www.spiegel.de/netzwelt/netzpolitik/e-evidence-warum-die-eu-plaene-zu-digitalen-beweisen-gefaehrlich-sind-a-1270939.html>.

⁶⁷⁹ EDPS. *EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters*, Opinion 7/2019, https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf, (6 November 2019). P. 19.

⁶⁸⁰ Burchard, C. [Christoph]. (2019). Europäische E-Evidence-Verordnung. *Zeitschrift für Rechtspolitik*, 2019(6), 164–167. P. 164.

⁶⁸¹ Burchard, C. [Christoph]. (2019). Europäische E-Evidence-Verordnung. *Zeitschrift für Rechtspolitik*, 2019(6), 164–167. P. 165.

⁶⁸² Burchard, C. [Christoph]. (2019). Europäische E-Evidence-Verordnung. *Zeitschrift für Rechtspolitik*, 2019(6), 164–167. P. 165.

⁶⁸³ <https://www.ccc.de/en>

⁶⁸⁴ European Digital Rights and Privacy International. (5 December 2018). *Growing concerns on “e-evidence”*: Council publishes its draft general approach. <https://edri.org/growing-concerns-on-e-evidence-council-publishes-draft-general-approach>.

To improve this situation, so-called “trilogues”⁶⁸⁵ were launched. For the Parliament, LIBE submitted its report in December 2020.⁶⁸⁶ It supported the E-Evidence Regulation version of 17 April 2018 in principle but required corrections: The orders for access to traffic and content data should be subject to stricter requirements and only be issued for crimes for which there is at least a three-year prison sentence. The LIBE report recommended to extend the deadline for emergency cases to 16 hours and added a written consent requirement when the issuing State is subject to the Art. 7 TEU procedure on the rule of law. Other improvements requested in the LIBE report were that data subjects would need to be informed by default, and any exceptions would need a judicial order, the personal data obtained through such order shouldn’t be reused for other proceedings, and data illegally obtained should be erased and not be admissible in courts. The information obligation should not only refer to data subjects but also include a mandatory notification to the “affected State” (if the State of residence of the person whose personal data are sought is other than the issuing State) and the “executing” State. The Council’s version was far from that comprehensive.⁶⁸⁷ Christakis found correctly that

notifying the Member State of residence of the person whose data are sought would be preferable for several reasons. Such a solution would find the right balance between the interest of the issuing authority (to access quickly digital evidence in order not to hinder criminal investigations) and the need for adequate safeguards to protect other values. The Member State of residence would be able to exercise its traditional protective functions concerning the human rights of the targeted individual [...] [and] would also help protect the fundamental interests of the Member State where these persons reside, such as the national security of the Member State of residence.⁶⁸⁸

This could permit to adapt in an appropriate way in the digital world protections that already existed in the physical world under MLAT systems.

Christakis also observed that “while the burden for affected States should be low and the “protecting human rights/sovereign interests benefit” for them and their populations should be high, law enforcement people involved in the e-evidence negotiations do not always seem to realize the importance of this mechanism and do not necessarily declare themselves willing to ensure this “responsibility to protect” function envisioned for them” by the LIBE report.⁶⁸⁹ However, he disagreed with the LIBE report’s concept to also notify the State which executes the order.

LIBE listed also special provisions on the criminal liability of journalists and the freedom of expression in other media under the law of the executing State, which might need to be considered; inquiries should also be compatible with fundamental rights. This concept would then allow rights of data subjects to be guaranteed by the executing State and, where applicable, the affected State. Other fundamental rights mentioned in the LIBE report are the *ne bis in idem* principle, dual criminality considerations, privileges and

⁶⁸⁵ Trilogues are negotiation meetings of the three EU legislative bodies involved in the legislative process - the Council, the Parliament, and the Commission – to reach an agreement in the legislative process.

⁶⁸⁶ European Parliament. *Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD), (11 December 2020).

⁶⁸⁷ E.g., it removed the fundamental rights-based ground for refusal which the SP could invoke if the execution of a European Production Order would violate the Charter.

⁶⁸⁸ Christakis, T. [Theodore]. (14 January 2019). *E-Evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead*. <https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/?cn-reloaded=1>.

⁶⁸⁹ Christakis, T. [Theodore]. (14 January 2019). *E-Evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead*. <https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/?cn-reloaded=1>.

immunities, including protections for medical and legal professions, freedom of press and freedom of expression; limitations to the use of data obtained, including rules on (in)admissibility of evidence and erasure of data obtained in breach of Regulation; and effective legal remedies not only in the issuing but also in the executing State in accordance with national law, including the possibility to challenge the legality of the order. The LIBE report also proposed a more appropriate role for SPs by abandoning the high sanctions of the Council in case of non-cooperation with such orders and by introducing an immunity from liability provision for consequences resulting from compliance with a European Production Order.

Unfortunately, commented the EDRI, the information of the judicial authorities of the State in which the data subject has its habitual place of residence according to this version of the E-Evidence Regulation only needs to be conducted “where it is clear” that the data subject lives in another country – a term that is undefined and imprecise.⁶⁹⁰ The EDRI therefore proposed a mandatory involvement of the State of residence of the data subject “when it’s known or could have been known that the person whose data is sought lives there”⁶⁹¹. Moreover, the opinion of the judicial authorities of the country of residence of the data subject in any given case would only be “duly taken into account”⁶⁹². The EDRI recommended that these authorities should be able to block infringing foreign orders and not to be only vaguely consulted. Lastly, EDRI questioned the proportionality of the EPOC. It argued that direct cooperation with SPs for law enforcement is not always necessary to prevent relevant electronic evidence from being removed by suspects. The EPOC-PR would be less intrusive and most likely sufficient to achieve that aim (similar to a “quick data freeze”). It therefore proposed the EPOC to be completely removed from the E-Evidence Regulation and that “law enforcement agencies use the EPOC-PR to quick-freeze data they believe could contain relevant electronic evidence. The acquisition of that data should be done through the safer channels of the EIO and MLATs”⁶⁹³.

The triilogue in May 2021 also failed to produce a breakthrough. One of the biggest differences still seemed to be that the parliamentary version provided for a notification obligation on the part of the judicial authorities, including a deadline of ten days to review and, if necessary, to reject the order from outside the EU. The Parliament insisted that in the case of transborder orders, local judicial authorities should decide on their legality. Commission and Council wanted to assign the assessment, and thus liability, directly to the SPs concerned.

Such a legal assessment by the SPs as to whether a data processing is lawful by disclosing personal data to authorities would have showed similarities with the shift of the duty to conduct a TIA to the SPs after *Schrems II*. This version of the E-Evidence Regulation also applied the traditional principle of mutual recognition but would have based this on cooperation with private actors. Tosza therefore correctly resumed that this would

create a new paradigm of relationship between law enforcement and private actors in a cross-border setting. The service provider replaces the state in being the recipient and first filter of requests coming from law enforcement in another state. The role of the

⁶⁹⁰ EDRI. (14 November 2019). *E-evidence: Repairing the unrepairable*. <https://edri.org/our-work/e-evidence-repairing-the-unrepairable>.

⁶⁹¹ EDRI. (14 November 2019). *E-evidence: Repairing the unrepairable*. <https://edri.org/our-work/e-evidence-repairing-the-unrepairable>.

⁶⁹² EDRI. (14 November 2019). *E-evidence: Repairing the unrepairable*. <https://edri.org/our-work/e-evidence-repairing-the-unrepairable>.

⁶⁹³ EDRI. (14 November 2019). *E-evidence: Repairing the unrepairable*. <https://edri.org/our-work/e-evidence-repairing-the-unrepairable>.

service provider is fundamental, as regardless of the declarations as to their function, they will not be able to abstain from a verification of the orders and questioning the validity of the abusive ones. While having to consider fundamental rights questions and even national interests potentially at stake, they become more of a public authority than a private actor in that respect. This role will however always be executed at a threat of being punished for non-compliance. [...] [This is] not a gradual evolution slightly intensifying cooperation, but a jump to a new level of trust, which comes at the time, where the whole concept of mutual trust is being questioned with higher intensity. Interestingly, this legal revolution comes at times of crisis in mutual trust between Member States regarding the level of judicial independence and safeguarding fundamental trust. This new system was conceived to solve the need for digital evidence in domestic cases, where the only cross-border element is the data being held by a foreign service provider. Yet at no point does the draft Regulation limit its application to these cases. Instead it creates a completely new model of cooperation in criminal matters with a significant role of a private actor.⁶⁹⁴

The European Parliament voted on 13 June 2023 to adopt the compromise text of the E-Evidence Regulation.⁶⁹⁵ Therein, E-Evidence is defined as subscriber data, traffic data, or content data stored by a SP in electronic form. The adopted version applies to TFPD cases, which are those in which a SP is established or represented in a Member State other than the law enforcement authorities issuing the order. A Preservation Order is limited to 60 days, a Production Order allows to compel SPs to produce data within 10 days, in emergency cases even within 8 hours. Non-compliance with these orders by a SP can lead to a fine of 2% of its total worldwide annual turnover of the preceding financial year. This brings another danger, which lies in the nature of a private actor: The SP could consider “what is more profitable (or less damaging) – comply with the request or risk sanctions”⁶⁹⁶, which contrasts with an independent handling of those cases by a judicial authority. The E-Evidence Regulation version of January 2023 triggered EDRi to specify its opinion from the end of 2019 in February 2023; we agree with this opinion. We think that such notification is necessary not only to resolve rule of law problems but also to give a solid legal basis to E-Evidence and to offer all Parties concerned the same rights to be informed; in particular because the executing State and the issuing State both have an obligation to protect the Charter and they can only abide to this obligation if they are equally informed about all facts of the order in question. EDRi commented that this January 2023 version removes the independent consideration of a second judicial authority from the scenario and therefore “reduces the notification mechanism to a trickle”⁶⁹⁷. EDRi therefore recommended a minimum safeguarding mechanism consisting of an obligation for notification

to (1) the judicial authorities where the person whose personal data is requested resides (the “affected State”) as they are best placed to know about their potential special protected status limiting access (a journalist, a lawyer, a social worker or a

⁶⁹⁴ Tosza, S. [Stanislaw]. (19 September 2019). *Mutual Recognition by Private Actors in Criminal Justice? Service Providers As Gatekeepers of Data and Human Rights Obligations*, <https://ssrn.com/abstract=3517878>. P. 20.

⁶⁹⁵ European Parliament. (13 June 2023). *Electronic evidence: new rules to speed up cross-border criminal investigations*. https://www.europarl.europa.eu/pdfs/news/expert/2023/6/press_release/20230609IPR96203/20230609IPR96203_en.pdf. // *Nota bene*: Our legal analysis is – in view of the version only recently adopted by the Parliament – only cursory analyzing the final text published by the Council in January 2023 (Council of the European Union, *Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings - Analysis of the final compromise text*, 5448/23, (20 January 2023). Also, as noted at the beginning of this work, the research for this thesis closed on 30 June 2023 and thus any subsequent development could not be taken into account.

⁶⁹⁶ Tosza, S. [Stanislaw]. (19 September 2019). *Mutual Recognition by Private Actors in Criminal Justice? Service Providers As Gatekeepers of Data and Human Rights Obligations*, <https://ssrn.com/abstract=3517878>. P. 20.

⁶⁹⁷ EDRi. (7 February 2023). *e-Evidence compromise blows a hole in fundamental rights safeguards*. <https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards>.

medical professional); (2) the judicial authorities in the “executing State”, where the company is officially located or established in order to guarantee legal certainty.⁶⁹⁸

In the version adopted by the Parliament in June 2023, this is implemented at least in part, but only in cases – more interfering with fundamental rights of the data subjects – for European Production Orders to obtain content- and traffic data; no notification is required for production orders regarding subscriber information “requested for the sole purpose of identifying the user”; no notification at all is required for preservation orders. Moreover, the affected State will not receive notification mechanism. This then leads to the fact that if the affected Member State does not coincide with the executing Member State, both do not include in their assessment the potentially affected rights of the data subject.

Moreover, the issuing Member State shall be exempt from notifying its counterpart if it has “reasonable grounds to believe that the offence is committed in the issuing State, and where the person whose data are sought resides in the issuing State”.

In this regard, EDRi correctly analyzed that

this “residency criteria” is extremely problematic because (1) this assessment is left entirely to the discretion of the issuing State’s investigative authority, which has considerable interests in avoiding the notification procedure perceived as ‘too cumbersome’ and the risk to have their order refused by the executing State, and (2) the factors that should guide the issuing State to make that assessment are excessively vague and can be easily twisted (the person has “family ties or economic connections” or “manifested the intention to settle in that Member State” or “established the habitual center of his or her interests in a particular Member State or has the intention to do”).⁶⁹⁹

A copy of a European Production Order is to be sent to a “competent authority” (in the executing Member State) where the SP is established. This authority then has 10 days or, in emergency cases, 4 days to express a ground for refusal. This final version leaves it to the Member States’ right to determine this authority and does not explicitly require that it be a judicial authority. Albus therefore correctly found that

the fact remains that henceforth the logic underlying cooperation requests will be reversed: instead of a judicial authority actively taking a decision on the recognition and execution of an order emanating from another Member State, automatic execution is now the rule, except where the competent authority chooses to intervene and raise a ground for refusal. This arrangement is fundamentally at odds with meaningful judicial oversight which is key to safeguarding fundamental rights in the context of extraterritorial enforcement of criminal law.⁷⁰⁰

Also, it is not clear from this version whether the authority in the executing Member State has a responsibility to assess the order, as Recital 42b says “it should have the right to assess”. Moreover, difficulties may arise in practice, because such an assessment can be burdensome for the executing State – we are hereby thinking of the unequal distribution of fines and cases within the Union⁷⁰¹ – and there are “doubts as to whether

⁶⁹⁸ EDRi. (7 February 2023). *e-Evidence compromise blows a hole in fundamental rights safeguards*. <https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards>.

⁶⁹⁹ EDRi. (7 February 2023). *e-Evidence compromise blows a hole in fundamental rights safeguards*. <https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards>.

⁷⁰⁰ Albus, V. [Valerie]. (15 June 2023). *Fast-Tracking Law Enforcement at the Expense of Fundamental Rights*. <https://verfassungsblog.de/fast-tracking-law-enforcement-at-the-expense-of-fundamental-rights>.

⁷⁰¹ See Chapter IX, Section I.1.1.

the notification requirement will be suited to uphold a high and uniform level of fundamental rights protection in practice”⁷⁰².

With Albus we also think that, overall, this version of the E-Evidence Regulation “was designed primarily with the interest of law enforcement authorities in mind. It is doubtful whether the purported advantages of direct cooperation will outweigh the risks of abuse and fundamental rights violations”⁷⁰³.

3.8. Digital Single Market Strategy and Data Strategy

Even though the hereafter mentioned two strategies break through the logical time sequence of the above-mentioned instruments, they should find its place in this thesis at this point. Both have in common that they are not a binding instrument of secondary law. Moreover, the Commission links the “Data Strategy” to the “Digital Single Markets Strategy”. Both showcase the tension between a need for a free TFPD and that of regulation, as already described in Chapter I. Therefore, both will be presented here as building on each other for better understanding.

3.8.1. Digital Single Market Strategy and Free Flow of Data Initiative

The former President of the Commission, Jean-Claude Juncker, announced in 2014 “that we must make much better use of the great opportunities offered by digital technologies, which know no borders. To do so, we will need to have the courage to break down national silos in telecoms regulation, in copyright and data protection legislation, in the management of radio waves and in the application of competition law”⁷⁰⁴. His agenda’s ideas were transformed into the “Digital Single Market Strategy”⁷⁰⁵. In 2017, the Commission published a paper titled “Building A European Data Economy”, accompanied by a working document.⁷⁰⁶ Both documents are part of the Digital Single Market Strategy and constitute the “Free Flow of Data Initiative”. Within the latter, the Commission found a lack of a comprehensive policy framework concerning raw machine-generated data that do not qualify as personal data.⁷⁰⁷ “Raw machine-generated data” concerns cases whenever SPs data generate data through their processes or machines, whereas the users have no direct access, even though they may be the owner of the machine.⁷⁰⁸ The scope of this thesis includes only TFPD but it is nevertheless important to note that these “free flow” elements were already recognized in 2014 and are also found in instruments such as the GDPR that apply only to personal data.

⁷⁰² Albus, V. [Valerie]. (15 June 2023). *Fast-Tracking Law Enforcement at the Expense of Fundamental Rights*. <https://verfassungsblog.de/fast-tracking-law-enforcement-at-the-expense-of-fundamental-rights>.

⁷⁰³ Albus, V. [Valerie]. (15 June 2023). *Fast-Tracking Law Enforcement at the Expense of Fundamental Rights*. <https://verfassungsblog.de/fast-tracking-law-enforcement-at-the-expense-of-fundamental-rights>.

⁷⁰⁴ European Commission. *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, (6 May 2015). P. 2.

⁷⁰⁵ European Commission. *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, (6 May 2015).

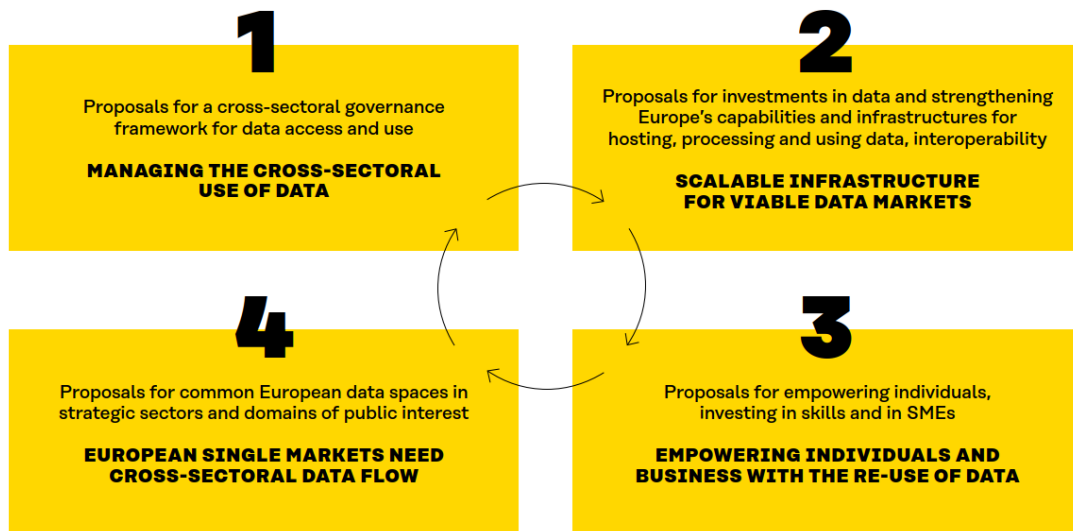
⁷⁰⁶ European Commission. *Building a European Data Economy*, COM(2017) 9 final, (10 January 2017). // European Commission, *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy*, SWD(2017) 2 final, (11 January 2017).

⁷⁰⁷ European Commission. *Building a European Data Economy*, COM(2017) 9 final, (10 January 2017). P. 10.

⁷⁰⁸ European Commission. *Building a European Data Economy*, COM(2017) 9 final, (10 January 2017). P. 10.

3.8.2. Data Strategy

The Commission formulated its first Data Strategy in 2010 with several key objectives.⁷⁰⁹ 10 years later, its strategy covers a range of different measures within four “blocks”.⁷¹⁰



Source: De Bièvre, M. [Matthias] et al., “35 proposals to make the European data strategy work”⁷¹¹

The Data Strategy aims to enable Europe adopt the latest digital technology, to strengthen its cybersecurity capacities and to become the “most attractive, most secure and most dynamic data-agile economy in the world”.⁷¹² The Commission announced that it would focus on three main objectives over the next five years: a fair and competitive digital economy, technology that works for people, and an open, democratic and sustainable society.⁷¹³ It also recognized a number of problems that prevent the Union from realizing their potential in the data economy: insufficient data availability, unequal market power, insufficient data governance, inadequate data infrastructures and technologies, especially in cloud markets, as well as inadequate interoperability and quality of data.⁷¹⁴ It also aimed at presenting an alternative to the platform business model dominated by large technology companies. This can be understood as the Commission’s wish to limit so-called “Very Large Online Platforms” (VLOPs)⁷¹⁵ such as Meta and Google, whose degree of market power arises from a “data advantage” and to

⁷⁰⁹ European Commission. *European Commission sets out strategy to strengthen EU data protection rules.* (4 November 2010). https://ec.europa.eu/commission/presscorner/detail/en/IP_10_1462.

⁷¹⁰ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data,* COM(2020) 66 final, (19 February 2020).

⁷¹¹ De Bièvre, M. [Matthias] et al. (2020). *35 proposals to make the European data strategy work.* Sitra. <https://www.sitra.fi/en/publications/35-proposals-to-make-the-european-data-strategy-work>. P. 3.

⁷¹² European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data.* COM(2020) 66 final (19 February 2020). P. 25.

⁷¹³ European Commission. (February 2020). *Shaping Europe's digital future.* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.

⁷¹⁴ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data,* COM(2020) 66 final, (19 February 2020). P. 6 ff.

⁷¹⁵ A VLOP is considered as “systemic in nature” and provides its services to an average of more than 45 million users per month, which corresponds to around 10 percent of the EU population. See European Commission. (10 May 2022). *Questions and Answers: Digital Services Act.* https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348.

prevent large market participants from determining the rules for the platform and unilaterally define conditions for data access and data usage.⁷¹⁶

The Commission's aim was to create a single European data space, which means an internal market for personal and non-personal data, in which these data are both secure and, as to industrial data, easily accessible to companies. On the one hand, this overarching strategy is intended to avoid fragmentation of the internal market due to inconsistent procedures between sectors or Member States; on the other hand, data should be able to be onwarded within the EU and across industries. The European regulations and values, in particular regarding data protection, consumer protection and competition, should be fully respected. The rules for data access and data use should also be fair, practicable and unambiguous, and there should be clear and trustworthy mechanisms for data governance. Ultimately, this should enable an "open, but assertive approach to international data flows, based on European values"⁷¹⁷.

One part of the Data Strategy is the "Data Governance Act" (DGA), which the Commission proposed in November 2020.⁷¹⁸ After the Parliament, the Council approved this proposal on 16 May 2022.⁷¹⁹ The DGA is intended to

create a mechanism to enable the safe reuse of certain categories of public-sector data that are subject to the rights of others. This includes, for example, trade secrets, personal data and data protected by intellectual property rights. Public-sector bodies allowing this type of reuse will need to be properly equipped, in technical terms, to ensure that privacy and confidentiality are fully preserved. In this respect, the DGA will complement the Directive from 2019, which does not cover such types of data.⁷²⁰

The DGA should also ease individuals "to allow the use of the data they generate for the public good, if they wish to do so ("data altruism"⁷²¹), in compliance with the GDPR"⁷²² and "support wider international sharing of data, under conditions that ensure compliance with the European public interest and the legitimate interests of data providers"⁷²³. The DGA may be considered as meant to regulate data intermediaries and in general as a "data economic law", thus a regime that recognizes data as an economic good and is committed to their better usability and tradability for the benefit of new technologies that depend on them.⁷²⁴ This could also serve to create trust in intermediaries that exchange

⁷¹⁶ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 8.

⁷¹⁷ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 5.

⁷¹⁸ European Commission. *Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, COM(2020) 767 final, (25 November 2020). ("DGA").

⁷¹⁹ Council of the EU. (16 May 2022). *Council approves Data Governance Act*.

<https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees>.

⁷²⁰ Council of the EU. (30 November 2021). *Promoting data sharing: presidency reaches deal with Parliament on Data Governance Act*. <https://www.consilium.europa.eu/en/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act>.

⁷²¹ Art. 2(10) DGA defines "data altruism" as "the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services". In addition, some general considerations about data altruism can be found in Art. 16 DGA.

⁷²² European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 13.

⁷²³ European Commission. (25 November 2020). *Commission proposes measures to boost data sharing and support European data spaces*. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2102.

⁷²⁴ See also Chapter X, Section III.

non-personal data under this governance framework.⁷²⁵ The DGA hereby wants to “create a framework to foster a new business model – data intermediation services – that will provide a secure environment in which companies or individuals can share data”⁷²⁶.

The proposed “Data Act”⁷²⁷ is the second deliverable resulting from the Commission’s Data Strategy. As the DGA “does not grant, amend or remove the substantial rights on access and use of data”⁷²⁸, this was left for the Data Act, which aims at complementing the DGA. While the DGA

creates the processes and structures to facilitate data sharing by companies, individuals and the public sector, the Data Act clarifies who can create value from data and under which conditions. Together, these initiatives will unlock the economic and societal potential of data and technologies in line with EU rules and values. They will create a single market to allow data to flow freely within the EU and across sectors for the benefit of businesses, researchers, public administrations and society at large.⁷²⁹

With the Data Act, the Commission intends “legislative action on issues that affect relations between actors in the data-agile economy to provide incentives for horizontal data sharing across sectors (complementing data sharing within sectors as described in the appendix)”⁷³⁰ which “aims to make the EU a leader in our data-driven society”⁷³¹. The Data Act includes therefore improved access to private sector data for the public sector, with a more flexible framework for requirements and safeguards for data access, to create intermediary structures to aggregate demand, and to bring together public sector entities interested in specific data and private sector data holders. A right to access privately held data is included, whereby this access to data should only be made mandatory in exceptional cases⁷³² and then at least under fair, reasonable, appropriate, and non-discriminatory conditions⁷³³. The Data Act interacts with other instruments. One is the “Open Data Directive”⁷³⁴; in this respect, “an implementing law is expected to be adopted in the coming months that will define a list of high-value datasets to be made available by the public sector free of charge and through application programming

⁷²⁵ As Mr. Koritnik, Minister for Public Administration for Slovenia expressed, “this will not oblige anyone to share their data, but for those who want to make their data available for certain purposes, it creates a safe and easy way to do it and to stay in control”. See Bertuzzi, L. [Luca]. (1 October 2021). *EU countries green light new data governance framework*. <https://www.euractiv.com/section/data-protection/news/eu-counties-green-light-new-data-governance-framework>.

⁷²⁶ Council of the EU. (16 May 2022). *Council approves Data Governance Act*. <https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees>.

⁷²⁷ European Commission. *Proposal for a Regulation of the European Parliament and the Council on harmonized rules on fair access to and use of data (Data Act)*, COM(2022) 68 final, (23 February 2022). (“Data Act”).

⁷²⁸ European Commission. *Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, COM(2020) 767 final, (25 November 2020). P. 1.

⁷²⁹ European Commission. (23 February 2022). *Data Act: Commission proposes measures for a fair and innovative data economy*. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

⁷³⁰ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 13.

⁷³¹ European Commission. (23 February 2022). *Data Act – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.

⁷³² European Commission. (23 February 2022). *Data Act: Commission proposes measures for a fair and innovative data economy*. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

⁷³³ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 13. // European Commission. (23 February 2022). *Data Act: Commission proposes measures for a fair and innovative data economy*. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

⁷³⁴ European Commission. *Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive)*, OJ L 172, 56–83, (26 June 2019). (“Open Data Directive”).

interfaces (APIs).⁷³⁵ The Data Act also “clarifies that the “Database Directive”⁷³⁶ cannot be used to prevent data generated by a connected product or related service from being accessed”⁷³⁷. The Data Act is consistent with the GDPR and strengthens the right to data portability “so that consumers can access and port any data generated by the product, both personal and non-personal”⁷³⁸.

The “Digital Services Act Package” includes the “Digital Services Act” (DSA)⁷³⁹ and the “Digital Markets Act” (DMA).⁷⁴⁰ There are similar initiatives on the US side.⁷⁴¹ Both Acts together aim at creating a new set of rules for all digital services, including social media, online marketplaces, and other online platforms that operate in the Union. They were depicted as “twin pieces of legislation at the heart of the European Commission’s push for greater independence from foreign digital giants”⁷⁴². The main distinction between the two in legislative intention is that the economic concerns associated with the collection of data by so-called “gatekeepers” are the subject of the DMA, while broader societal concerns are addressed in the DSA. Data protection is not the central topic of the DSA. The Union is placing a greater focus on data protection in its accompanying legislative initiatives (DGA). Nevertheless, all three Acts together will improve the level of protection for data subjects. Although particularly the DMA has a competition law focus rather than a human rights focus, its consideration in this thesis is relevant because markets created by exploiting personal data are particularly attractive to companies, given the potential returns. There is therefore a strong competition for those markets. Consumers initially benefit from this in the form of more innovation and better conditions. However, once a company established a position of power, disadvantages are possible from the consumer’s point of view; this includes the increasing collection of personal data and that consumers could be locked into the ecosystem of a single, market-dominant company (so-called “lock-in effects”)⁷⁴³. The EU wanted to compensate for these disadvantages through the GDPR and accompanying interventions under competition and antitrust law. Data protection investigation thus can complement the antitrust scrutiny of VLOPs business’ in Europe. The Commission’s Digital Services Act Package therefore

⁷³⁵ European Commission. (23 February 2022). *Data Act – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.

⁷³⁶ European Commission. *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases*, OJ L 077, 20–28, (27 March 1996). (“Database Directive”).

⁷³⁷ European Commission. (23 February 2022). *Data Act – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.

⁷³⁸ European Commission. (23 February 2022). *Data Act – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.

⁷³⁹ European Commission, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, OJ L 277, 1–102, (27.10.2022). (“Digital Services Act”). // *Nota bene*: This analysis is based on the proposed text of the DSA (European Commission. *Proposal for a Regulation of the European Commission and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, COM(2020) 825 final, (16 December 2020)).

⁷⁴⁰ European Commission, *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*, OJ L 265, 1–66, (12 October 2022). (“Digital Markets Act”). // *Nota bene*: This analysis is based on the proposed text of the DMA (European Commission. *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, COM(2020) 842 final, (15 December 2020)).

⁷⁴¹ The White House. *Executive Order on Promoting Competition in the American Economy*. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy>, (9 July 2021). // U.S. Chamber of Commerce. (17 June 2022). *Striking Similarities: Comparing Europe’s Digital Markets Act to the American Innovation and Choice Online Act*. <https://www.uschamber.com/finance/antitrust/striking-similarities-dma-american-innovation-act>.

⁷⁴² Politico. (14 December 2020). *Inside the EU’s divisions on how to go after Big Tech*.

<https://www.politico.eu/article/margrethe-vestager-thierry-breton-europe-big-tech-regulation-digital-services-markets-act>.

⁷⁴³ “Lock-in effects can be described as conditions in which a strong market participant (here: having a monopoly-like position because of the factual access to data plus having the technical means to protect the data from access by third Parties, which leads to factual exclusivity) is capable of making it at least very difficult for its contractual partners to switch to another supplier/provider.” Steinrötter, B. [Björn]. (2020). *Legal Framework for Commercialization of Digital Data*. In M. [Martin] Ebers and S. [Susana] Navas (eds.), *Algorithms and Law* (pp. 269–298). Cambridge University Press. P. 272–273. P. 273.

complements the Union's tendency to find other ways and means besides the GDPR to urge VLOPs to maintain compliance.

The DSA amends the E-Commerce Directive⁷⁴⁴ and is intended to harmonize rules for SPs. The DSA defines in Chapter II the liability exemptions of SPs and sets due diligence obligations in Chapter III. Like the platform-to-business regulation (P2B Regulation)⁷⁴⁵, the obligations set by the DSA are scaled according to nature and size of the platform. The larger a platform of a SP is, the more responsibility it has. "Certain substantive obligations are limited only to VLOPs, which due to their reach have acquired a central, systemic role in facilitating the public debate and economic transactions. Very small providers are exempt from the obligations altogether"⁷⁴⁶. DSA covers in particular VLOPs such as Google, Meta and Microsoft. All those who offer their services in the internal market need to comply with the new rules, regardless of whether they are based in or outside the EU. The DSA therefore has an extraterritorial reach like the GDPR. The DSA requires a systematic risk management and yearly publication of a clear, easily understandable, and detailed report of the content moderation the SPs have carried out during the relevant period. Measures of this moderation can be, for example, stops of advertising payments for relevant content or an expanded visibility of reliable information sources. These reports must also include algorithmic decisions and their human control, so that users can control which content is displayed. The SPs, however, are allowed to assess themselves the risks their services entail, which could endanger fundamental rights, such as the freedom of speech and information, the right to data protection, and the right to non-discrimination. Art. 16 DSA provides for the establishment of the principle – familiar from the E-Commerce Directive – of "notice-and-action". An obligation to delete data therefore only exists when the SP has been notified of an infringement or otherwise becomes aware of it. SPs are also required to introduce user-friendly procedures that enable users to report illegal content. Transparency requirements encompass that advertising must be clearly marked as such. In addition, the name of the natural or legal person on whose behalf the advertisement is displayed must be stated. Furthermore, the DSA now requires the disclosure of meaningful information about the most important parameters for determining the users to whom the advertising is displayed. Likewise, it must be indicated when profiling is used. This allows users to better understand who is behind an advertisement and why it is being displayed to him or her. SPs must also ensure that users can adjust these parameters – including the option to switch off individually tailored feeds. To avoid liability, platforms must prove that they have no actual knowledge of illegal content on their pages or that they acted immediately to remove the content or to block access to it. The enforcement of the regulation is regulated in Chapter IV. It requires VLOPs to appoint qualified compliance officers, so-called "Digital Services Coordinators" in each Member State, and the creation of a so-called "European Board for Digital Services". The DSA also empowers the SAs to impose severe penalties on online services for violations of the law. In addition to periodic penalty payments and interim measures, the DSA also provides for fines of up to 6% of a company's prior-year revenue.

The DMA is intended to ensure the "contestability" of all online services, whilst contestability can be harmed by an oligopoly of gatekeepers. It "ban[s] certain practices used by large platforms acting as gatekeepers and enable the Commission to carry out

⁷⁴⁴ See Chapter II, Section II.3.2.

⁷⁴⁵ European Commission. *Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services*, OJ L 186, 57–79, (11 July 2019). ("P2B Regulation").

⁷⁴⁶ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, COM(2020) 842 final, (15 December 2020). P. 6.

market investigations and sanction non-compliant behavior”.⁷⁴⁷ Such gatekeepers are defined according to certain quantitative thresholds. A company must operate one or more central platform services in at least three Member States and have, over the past three financial years, generated annual sales of at least EUR 7.5 billion in the Union or its stock market value is at least EUR 75 billion and it has at least 45 million monthly active end users established or located in the Union and at least 10,000 yearly active business users established in the Union. Nevertheless, the Commission also has powers to designate companies as gatekeepers following a market investigation. This allows emerging gatekeepers to be captured by the scope of the DMA if their competitive position has been demonstrated but is not yet permanent. This prohibits a number of practices which are unfair, whilst unfairness relates to “an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage”⁷⁴⁸. The DMA requires gatekeepers “to proactively put in place certain measures, such as targeted measures allowing the software of third Parties to properly function and interoperate with their own services”⁷⁴⁹. Gatekeepers’ services have to respect fair, reasonable and non-discriminatory access to their services for business users. The DMA also contains some data protection provisions, including the prohibition of (a) processing for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper; (b) combining personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services; (c) cross-using personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa; and (d) sign in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and has given consent within the meaning of Article 4(11) and Article 7 GDPR, and without prejudice for the gatekeeper to rely on the legal bases of Art. 6(1) (c), (d) GDPR, where applicable.⁷⁵⁰

The Data Strategy aims at the creation of a “genuine single market for data, as well as ten sectoral common European data spaces that are relevant for the twin green and digital transitions”.⁷⁵¹ EU-wide interoperable data spaces in strategic sectors are foreseen for 10 strategic fields: health, agriculture, manufacturing, energy, mobility, financial, public administration, skills, the European Open Science Cloud and the crosscutting priority of meeting the “Green Deal”⁷⁵² objectives.

⁷⁴⁷ European Parliament. (24 March 2022). *Deal on Digital Markets Act: EU rules to ensure fair competition and more choice for users*. <https://www.europarl.europa.eu/news/de/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users>.

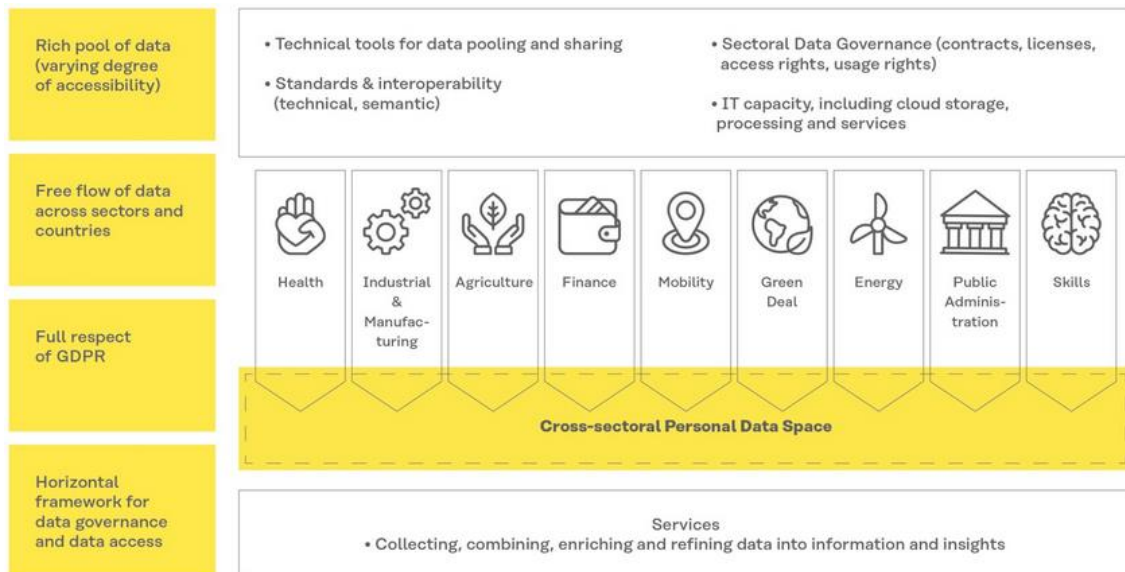
⁷⁴⁸ Recital 33 of the DMA.

⁷⁴⁹ European Commission. (15 December 2020). *Europe fit for the Digital Age: Commission proposes new rules for digital platforms*. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2347.

⁷⁵⁰ Art.5(2) DMA.

⁷⁵¹ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 2.

⁷⁵² European Commission. (2023). *A European Green Deal*. https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.



Source: De Bièvre, M. [Matthias] et al., “35 proposals to make the European data strategy work”⁷⁵³

Herewith, the EU wants to escape from the dependence on US cloud providers, develop the fragmentation of the European digital economy and rely on decentralized “edge computing”⁷⁵⁴ instead of Cloud Computing systems. The Commission therefore presented an initiative to “draw up rules for common European data spaces (covering areas like the environment, energy and agriculture) to make better use of publicly held data for research for the common good, support voluntary data sharing by individuals and set up structures to enable key organizations to share data”⁷⁵⁵ and “supports the development of data spaces through its funding programs (Digital Europe Programme, Horizon Europe, Connecting Europe Facility). Stakeholders in the data economy are encouraged to build up data spaces. The Commission will further report on the development of common European data spaces in 2023”⁷⁵⁶. Until then, however, data spaces got even less attention than the DGA – with the health data space⁷⁵⁷ being an exception. The question is also which data should be processed in these data spaces and whether the EU wants to build such data space in order not to repeat the weakness⁷⁵⁸ of signing the EU-US TFTP agreement⁷⁵⁹. This agreement allows transfers of EU data to the US (Treasury Department) to perform an analysis of these data there and to send the results back to the EU (Europol). Without having its own data space, the

⁷⁵³ De Bièvre, M. [Matthias] et al. (2020). *35 proposals to make the European data strategy work*. Sitra. <https://www.sitra.fi/en/publications/35-proposals-to-make-the-european-data-strategy-work>. P. 11.

⁷⁵⁴ Processing systems close to the consumer, ideally using the user's own system.

⁷⁵⁵ European Commission. (2021). *Data sharing in the EU – common European data spaces (new rules)*. <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Legislative-framework-for-the-governance-of-common-European-data-spaces>.

⁷⁵⁶ European Commission. (23 February 2022). *Data Act – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.

⁷⁵⁷ European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, 2022/0140(COD), (3 May 2022).

⁷⁵⁸ “When the EU reluctantly agreed to the TFTP agreement, there was a widespread sense of unease in Brussels about relying on the United States for counterterrorism analysis of data located on European soil. Indeed, the TFTP agreement itself cited “the possible introduction of an equivalent EU system allowing for a more targeted transfer of data”. In 2013, the European Commission dutifully prepared the ground for legislation, but a European TFTP never got off the ground.” See The Lawfare Institute. (14 December 2020). *The Latest Skirmish in the Transatlantic Data Wars*. <https://www.lawfareblog.com/latest-skirmish-transatlantic-data-wars>.

⁷⁵⁹ European Commission. *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, OJ L 195, 5–14, (27 July 2010). // The Council of the EU. 2010/412/: *Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, OJ L 195, 3–4, (27 July 2010).

EU back then “effectively deputized the U.S. Treasury to perform counterterrorism searches of European data: The U.S. service is free and fast, and it yields actionable intelligence, all while avoiding the inevitable privacy law complications that would have limited the scale and effectiveness of a European version of the system.”⁷⁶⁰

A central point is also a necessary infrastructure on which data are to be exchanged and processed. There are already various initiatives in Member States heading towards a “Federated Data Infrastructure for European ecosystems”, for example “Gaia-X” in Germany, “*Cloud de Confiance*” in France, or the “International Data Spaces” initiative⁷⁶¹ which aims at cross-sectoral data sovereignty and data interoperability. The German federal government is in an exchange with the EU Commission and various EU Member States regarding its data infrastructure project “Gaia-X”. The project and the initiatives of the EU Commission could complement each other well, explained the German Federal Government.⁷⁶² This example shows that a European strategy must be coordinated with possible parallel running projects of Member States. The Commission announced that it intends to adopt a “Memorandum of Understanding” with the Member States. These data spaces “are to be supported by the European cloud federation, providing data processing and cloud infrastructure services compliant with the GDPR. The GDPR ensures a high level of protection of personal data and a central role for individuals in all these data spaces while providing the necessary flexibility to accommodate different approaches.”⁷⁶³ These infrastructural measures also include the draft “Cybersecurity Certification Scheme for Cloud Services” (EUCS)⁷⁶⁴, which looks into cybersecurity certification of cloud services. The EUCS is a voluntary scheme⁷⁶⁵ and secondary legislation under the “Cybersecurity Act” (EUCSA)⁷⁶⁶, which introduced an EU-wide cybersecurity certification framework for information and communications technology products, services and processes, aiming to increase trust and security in those. The EUCS stipulates that “the objective of these specific requirements is to adequately prevent and limit possible interference from states outside of the EU with the operation of certified cloud services”. The EUCS also has an effect of data localization to be discussed below⁷⁶⁷. In addition to the technical / infrastructural focus of the EUCS, it is nevertheless suspected that “these requirements have nothing to do with cybersecurity concerns, some may even argue this is a protectionist approach pushed by certain national governments”⁷⁶⁸.

⁷⁶⁰ The Lawfare Institute. (14 December 2020). *The Latest Skirmish in the Transatlantic Data Wars*. <https://www.lawfareblog.com/latest-skirmish-transatlantic-data-wars>.

⁷⁶¹ International Data Spaces Association. (April 2020). *Implementing the European Strategy on Data. Role of the International Data Spaces (IDS), Position Paper*. <https://internationaldataspaces.org/wp-content/uploads/IDSA-Position-Paper-Implementing-European-Data-Strategy-Role-of-IDS1.pdf>.

⁷⁶² Deutscher Bundestag. (9 January 2020). *Umsetzung und Zeitplanung von “GAIA-X”*. <http://dip21.bundestag.de/dip21/btd/19/164/1916434.pdf>. P. 3.

⁷⁶³ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 2.

⁷⁶⁴ EU Agency for Cybersecurity. (22 December 2020). *EUCS – Cloud Services Scheme*. <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>.

⁷⁶⁵ Although “experts expect the certification to become mandatory in the future”. See Kabelka, L. [Laura]. (16 June 2022). *Sovereignty requirements remain in cloud certification scheme despite backlash*. <https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash>.

⁷⁶⁶ European Commission. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, OJ L 151, 15–69, (7 June 2019).

⁷⁶⁷ Chapter VIII, Section III.

⁷⁶⁸ Kabelka, L. [Laura]. (16 June 2022). *Sovereignty requirements remain in cloud certification scheme despite backlash*. <https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash>.

4. EU agreements with third countries or international organizations

The recognition of the EU as a subject of international law is a fundamental prerequisite for the Union's ability to act at the international level. Art. 47 TEU stipulates that the EU has legal personality. However, this personality is limited in functional aspects because it is derived from the Member States and its scope is based on the principle of individual authorization. This means that while the EU is in principle empowered⁷⁶⁹ to conclude international agreements, the conclusion itself is pending on the fact that the respective contractual basis allows membership of other international organizations. Being a subject in international law means the ability to bear the rights and obligations of international law. The EU can thus be claimed for the violation of international obligations. Conversely, this also applies to their right to assert an infringement by another contracting Party.

Title V of the TFEU regulates competencies and procedures for concluding agreements. Art. 216(2) TFEU clarifies that the agreements concluded pursuant to para. 1 are binding for the institutions of the Union and its Member States. The procedure provides for the Parliament's consent to the Council decision, Art. 218(6) TFEU. Regarding international contract law, Art. 216(2) TFEU implies priority over secondary law. Since international agreements concluded by the EU are binding for the Union institutions, those must also adhere to their requirements if they enact secondary law.

The question remains as to whether the EU is also bound by international custom (or even the general principles of law)⁷⁷⁰. In contrast to international agreements, which bind the Union and the Member States under Art. 216(2) TFEU, EU primary law does not expressly regulate the question if the EU is bound by international custom. Case law of the CJEU⁷⁷¹ and researchers' opinions⁷⁷² assume that this second source of international law are also an integral part of the Union's legal order; nevertheless, the question of direct effect is unclear. The CJEU established that EU institutions can be found to violate them only when: (1) The rules of customary international law invoked are "fundamental," and (2) by adopting the suspending act, the EU institution made a manifest error of assessment concerning the conditions for applying those rules.⁷⁷³ Konstadinides therefore speculated "that although custom constitutes a useful source of inspiration for the CJEU, its role as a means of judicial review is still relatively small. [...] A private party may only be able to rely on customary international law in four circumstances"⁷⁷⁴. These are, that

⁷⁶⁹ Art. 3(5) TEU provides that "the EU shall uphold and promote [...] the strict observance and the development of international law".

⁷⁷⁰ "Case law of the CJEU is somewhat cryptic on the relationship (i.e., monist or dualist) between the EU legal order and custom or the general principles of international law. The EU's dualist approach to international law with reference to international treaties does not imply that the same occurs *ipso jure* with regard to customary international law. A glance at Article 3 (5) of the TEU and Article 218 of the TFEU suggests perhaps the opposite about customary international law—that the EU has adopted a monist approach." See Konstadinides, T. [Theodore]. (2012). When in Europe: Customary International Law and EU Competence in the Sphere of External Action. *German Law Journal*, 13(11), 1177–1202. P. 1180.

⁷⁷¹ CJEU. Judgment of the Court of 16 June 1998, *A. Racke GmbH & Co. v Hauptzollamt Mainz*, C-162/96, ECLI:EU:C:1998:293, (16 June 1998). Paras. 45 f. // CJEU. Judgment of the Court (Grand Chamber) of 3 June 2008, *The Queen, on the application of International Association of Independent Tanker Owners (Intertanko) and Others v Secretary of State for Transport*, C-308/06, ECLI:EU:C:2008:312. Para. 51 // CJEU. Judgment of the Court of 24 November 1992, *Anklagemyndigheden v Peter Michael Poulsen and Diva Navigation Corp*, C-286/90, ECLI:EU:C:1992:453. (24 November 1992). Para. 9

⁷⁷² Holdgaard, R. [Rass]. (2008). *External Relations Law of the European Community*. Wolters Kluwer. P. 179 ff. // Denza, E. [Eileen]. (2008). A note on Intertanko, *European Law Review* 33, 870-879. P. 875.

⁷⁷³ CJEU. Judgment of the Court of 16 June 1998, *A. Racke GmbH & Co. v Hauptzollamt Mainz*, C-162/96, ECLI:EU:C:1998:293. Paras. 48–49.

⁷⁷⁴ Konstadinides, T. [Theodore]. (2012). When in Europe: Customary International Law and EU Competence in the Sphere of External Action. *German Law Journal*, 13(11), 1177–1202. P. 1197–1198.

rules of customary international law invoked to challenge an EU legislative act must be fundamental [...], EU legislature has to make a manifest error of assessment concerning the conditions of applying the rules of customary international law invoked [...], principles of customary international law invoked are calling into question the competence of the EU to adopt the challenged EU legislative act [...], and the EU legislative act challenged is liable to affect rights which the individual derives from EU law or creates obligations under EU law.⁷⁷⁵

Ultimately, the binding of the EU to international custom results from its international subjectivity. In addition to the treaty making power, this also implies the binding nature of international custom and the general principles of law. This justification is of international law nature since it ties in with the membership of the EU in the international community. It is then obligatory from the perspective of international law that subjects of international law must abide by their rules, to ensure that the international legal framework for those who are the bearers of international law rights and obligations, is applicable. It therefore seems self-evident that the EU is bound, for example, by international custom or the principles of territorial sovereignty and integrity.

Obligations under the GDPR and other acts of the Union may conflict with the right of foreign public authorities to request the “production” of personal data. If, for example, a data processor who is also subject to the law of a country other than a Member State is requested to produce personal data, a production order could result in a violation of the data processing contract, but in particular also of the domestic law of the third country.⁷⁷⁶ If the data exporter knows of the possibility of such production order from authorities, and if this threatens the essentially equivalent level of data protection (requirement manifested in the *Schrems II* judgment), the conclusion of a data processing contract with such a company may be inadmissible due to the conscious acceptance of a possible interference with Union data protection law.

The EDPB stressed therefore that

in line with the CJEU case law, the obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness. It is therefore essential that EU negotiating Parties ensure that the provisions laid down in the additional protocol do comply with the EU *acquis* in the field of data protection in order to ensure its compatibility with EU primary and secondary law.⁷⁷⁷

The EU Commission therefore declared in its European Data Strategy, that it wants to take steps to address these concerns through international cooperation, such as the proposed EU-US agreement to facilitate transborder access to electronic evidence,⁷⁷⁸ or also working at the multilateral level within the framework of the Council of Europe, reduce the risk of legal conflict and provide clear safeguards for the data of EU citizens

⁷⁷⁵ Konstadinides, T. [Theodore]. (2012). When in Europe: Customary International Law and EU Competence in the Sphere of External Action. *German Law Journal*, 13(11), 1177–1202. P. 1199.

⁷⁷⁶ Such powers of intervention exist e.g., in the US due to the regulations to be analyzed below in Chapter III, Section II.; concerns were also raised by the Commission about several Chinese laws on cybersecurity and national intelligence. See European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 9.

⁷⁷⁷ EDPB. *Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)*, https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_en, (2 February 2021). P. 3.

⁷⁷⁸ See Chapter II, Section II.3.8.2.

and businesses, whereby a high level of protection of fundamental and procedural rights must be preserved.⁷⁷⁹

One possibility in that frame of international cooperation could be a “legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, based on that assessment, considers that appropriate safeguards with regard to the protection of personal data exist”.⁷⁸⁰ The term “legally binding instrument” is a Union law word creation from current data protection law. Directive 95/46 did not yet contain such a term. It is also not defined in the GDPR and the LED. The term usually refers to binding legal effects and obligations from a contract or other legal instruments. The Recitals of the LED place certain qualitative requirements on these legal instruments. These include legally binding bilateral agreements, such as MLATs, which have been concluded by the Union or a Member State and recognized as legally binding. Data subjects must also be able to enforce their rights. In particular, it should be ensured in this context that the data protection regulations and the rights of the data subjects, including their right to effective administrative and judicial remedies, are observed.⁷⁸¹

4.1. SWIFT Agreements

Since 2006, SWIFT provided the US Treasury Department with personal data in international money transfers.⁷⁸² US-EU negotiations became necessary because SWIFT's data center moved from the US to Switzerland, which made a domestic access by US authorities impossible. To diminish raised concerns, SWIFT concluded with the US Treasury Department a memorandum of understanding which narrowed the scope of TFPD to specific counter-terrorism cases, and subjected such transfers to independent oversight and audit, including real-time monitoring.⁷⁸³ Through the SWIFT interim agreement, US authorities were allowed to access personal data on transfers and other private banking account data of EU citizens to identify suspected terrorists. Any further use of this data required the US to justify this with identification, detection, prevention, or prosecution of terrorist financing. At the sight of the information about the data production requests by US authorities, leaked by Edward Snowden and others, it was questionable if the US authorities used this data for counterterrorism activities only.⁷⁸⁴ Under the pressure from members of the EP, the Council renegotiated with the US on the transfer of banking data in 2009.

⁷⁷⁹ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 9.

⁷⁸⁰ LED. Recital 71.

⁷⁸¹ LED. Recital 71.

⁷⁸² Meller, P. [Paul]. (22 September 2003). Europe Fights U.S. Over Passenger Data. *The New York Times*. <http://www.nytimes.com/2003/09/22/business/worldbusiness/22FLY.html?pagewanted=1>.

⁷⁸³ E.g., WP29 stated that even in the fight against terrorism and cybercrime the fundamental rights must be preserved. Article 29 Working Party. (23 November 2006). *Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2006/pr_swift_affair_23_11_06_en.pdf. P. 2.

⁷⁸⁴ dpa Deutsche Presse Agentur GmbH. (19 January 2010). *Illegale Überwachung: FBI erschlich sich Telefondaten zur Terrorabwehr. Der Spiegel*. <http://www.spiegel.de/politik/ausland/illegale-ueberwachung-fbi-erschlich-sich-telefondaten-zur-terrorabwehr-a-672646.html>.

After the Parliament rejected this new transatlantic SWIFT agreement in February 2010,⁷⁸⁵ the Parliament approved the revised agreement on 8 July 2010,⁷⁸⁶ which entered into force on 1 August 2010. Based on this, retrieved personal data are fed into the “Terrorist Finance Tracking Program” (TFTP) and evaluated. Affected data are name, account number, address, recipient and amount of a transfer for transactions to countries outside the EU and payments from such countries. The former EDPS Peter Hustinx criticized the new agreement and called for further improvements.⁷⁸⁷ He welcomed the fact that a narrower definition of terrorism and stronger safeguards for the data protection rights of citizens have been included. However, Hustinx also emphasized that there are still shortcomings. He proposed a clearer definition of the purpose of the agreement and was concerned about the plan to allow large amounts of banking information to be sent to US authorities. Improvements are also needed in terms of retention periods, enforceability of data protection rights for citizens, judicial supervision, and independent control. The Parliament subsequently – so far without the necessary conditional approval of the EU member states – demanded SWIFT to be suspended following allegations of Internet surveillance by US authorities.⁷⁸⁸

4.2. PNR Agreements

The transfer of PNR by European airlines to the US goes back to 2001. Following the 9/11 attacks, the US passed laws requiring airlines that fly to, from, or across the US to give US customs officials electronic access to the data of their reservation and check-in systems. EU parliamentarians criticized that the agreement between the Commission and the US also allows TFPD to third countries and that EU citizens are not protected against misuse of those data in the US, especially if e-mail addresses and credit card numbers were transmitted.

The CJEU annulled a corresponding agreement in 2006.⁷⁸⁹ It found that the agreement had to be based on the third pillar of the European Community (justice and home affairs), but at that time the Commission had chosen its internal market regulatory competence to conclude this agreement. Nevertheless, the CJEU did not comment on the material problems that were already present at the time.

Government officials from the EU and the US then agreed on an interim agreement which expired on 31 July 2007 and was replaced by a long-term agreement signed in July 2007.⁷⁹⁰ In this 2007 agreement, PNRs are stored by default in the US for fifteen years instead of three and a half. After the entry into force of the Treaty of Lisbon, the Parliament, which since then has a veto right also for international agreements in the area of cooperation in criminal matters, demanded a renegotiation of the 2007 agreement. Based on this, the Commission outlined the basis for PNR to third

⁷⁸⁵ European Parliament. (11 February 2010). *SWIFT: European Parliament votes down agreement with the US*. <http://www.europarl.europa.eu/sides/getDoc.do?language=en&type=IM-PRESS&reference=20100209IPR68674>.

⁷⁸⁶ EU. *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program*, OJ L 195, 5-14, (27 July 2010).

⁷⁸⁷ EDPS. (22 June 2010). *EU-US new draft agreement on financial data transfers: EDPS calls for further data protection improvements*. https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2010-10_tftp_agreement_en.pdf.

⁷⁸⁸ European Parliament. (22 October 2013). *EP to vote on suspending SWIFT deal after committee vote on data protection*. <http://www.europarl.europa.eu/news/en/news-room/20131021STO22709/EP-to-vote-on-suspending-SWIFT-deal-after-committee-vote-on-data-protection>.

⁷⁸⁹ CJEU. Judgment of the Court (Grand Chamber) of 30 May 2006, *European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities*, C-318/04, ECLI:EU:C:2006:346.

⁷⁹⁰ European Commission. *Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)*, OJ L 204, 16–25, (4 August 2007).

countries.⁷⁹¹ The Commission wanted to use a push system in the future, in which airlines transmit personal data to law enforcement agencies, whereas until now the airline authorities had to grant direct access to the PNR.

The Commission presented a new proposal in 2011.⁷⁹² On 19 April 2012, the Parliament voted in favor of this agreement with the US.⁷⁹³ Under this agreement, US authorities can store PNR for up to five years. After six months, however, anonymization of personal data is foreseen. After these five years, personal data can be stored for up to a further ten years, but US authorities will only have access to it under certain conditions. After this period, personal data are to be completely anonymized. Information needed for a specific case will be kept in the PNR database until a criminal investigation is completed and archived, which could theoretically lead to indefinite retention of PNR.

In July 2012, a new agreement for the transfer of air passenger data to Australian authorities was approved.⁷⁹⁴ The agreement provides that PNR can be stored in Australia for five and a half years and analyzed to combat terrorism and serious international crimes. After three years, the personal reference to the data is to be disguised. However, access to the full PNR remains possible in special cases. Particularly sensitive data relating to the ethnic origin, political conviction, belief, health or sexual life of a person concerned should be sorted out according to the presentation of the Council. The agreement also provides for the right to inspect and, where appropriate, correct or delete false information from EU citizens.

The envisaged PNR agreement between the EU and Canada provided that personal data can be saved for five years in the case of flights between Canada and the EU. The Council asked the Parliament to approve the agreement. After public pressure, the Parliament decided to have the agreement reviewed by the CJEU.⁷⁹⁵ It was the first time that the CJEU had to rule on the compatibility of a planned international agreement with the Charter. This occurred under influence of a CJEU ruling, which declared the Data Retention Directive to be invalid.⁷⁹⁶ In his closing plea, former Attorney General Paolo Mengozzi criticized the agreement on the exchange of PNR between Canada and the EU as incompatible with fundamental rights.⁷⁹⁷ One of his main arguments were possible onward TFPD through Canada to other States without being checked by an independent authority. He also addressed that the agreement would allow Canada to use these personal data for purposes other than safeguarding public security. In its opinion of 26

⁷⁹¹ European Commission. *Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries*, COM(2010) 492, (24 September 2010).

⁷⁹² European Commission. *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011)32, (8 February 2011).

⁷⁹³ European Commission. *Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security*, *Official Journal of the European Union*, L 215, 5–14, (11 August 2012).

⁷⁹⁴ European Commission. *Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service*, OJ L 186, 4–16, (14 July 2012).

⁷⁹⁵ European Parliament. (25 November 2014). *MEPs refer EU-Canada air passenger data deal to the EU Court of Justice*. <http://www.europarl.europa.eu/news/en/press-room/20141121IPR79818/meps-refer-eu-canada-air-passenger-data-deal-to-the-eu-court-of-justice>.

⁷⁹⁶ In its ruling of 8 April 2014, the CJEU had annulled Directive 2006/24/EC. The CJEU did not consider data retention to be fundamentally impermissible, but only possible under certain conditions and in compliance with the principle of proportionality: “the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52 (1) of the Charter”. See CJEU. Judgment of the Court of 8 April 2014, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

⁷⁹⁷ CJEU. Judgment of the Court of 8 April 2014, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others*, joined cases C-293/12 and C-594/12, Opinion of the Advocate General Mengozzi delivered on 8 September 2016, ECLI:EU:C:2016:656.

July 2017, the CJEU declared that the agreement could not be concluded in its intended form because some of its provisions did not meet the requirements stemming from the Charter.⁷⁹⁸ In principle, without excluding categorically the use of PNR data for security purposes, the CJEU found that both the transfer of PNR data from the Union to Canada and the rules contained in the envisaged agreement for the storage, use and possible transfer of the data to Canadian, European, or foreign authorities interfere with the fundamental right to respect for private life, and that the proposed agreement also interferes with the fundamental right to the protection of personal data. Further negotiations with Canada on a revised text “concluded successfully in March 2019 and the finalization of the agreement is currently pending its legal review and political validation by Canada.”⁷⁹⁹

Other ongoing negotiations for PNR Agreements are taking place with Japan. Former Commission President Jean-Claude Juncker announced in 2019 to negotiate with Japan on the use of PNR.⁸⁰⁰ On 18 February 2020, the Council adopted a decision authorizing the opening of negotiations between the Commission and Japan.⁸⁰¹ The agreement between the EU and Japan is intended to set the conditions for the exchange of PNR data with full respect for fundamental rights in accordance with the Charter.⁸⁰² Negotiations with Mexico, launched in July 2015, are currently at a standstill.⁸⁰³

The PNR agreements with Australia and the US contain provisions similar to those contested by the CJEU in the EU-Canada PNR agreement and therefore require review. This applies in particular to the categories of data that can be transmitted, to the transmission of sensitive data, to the transfer to third countries or the exceptional use of data for purposes other than security. A Union’s position made public in 2019 underlined the Union’s intention to promote the inclusion of several key data protection principles – similar to those of the GDPR – in the standards to ensure their compatibility with the EU legal regime.⁸⁰⁴

At its meeting on 7-8 June 2021, the Justice and Home Affairs Council adopted conclusions in particular on the PNR agreements with Australia and the US. It found that the agreements with Australia and US do not fully comply with the CJEU’s Opinion 1/15 that toppled the envisaged EU-Canada PNR deal because it was not in line with the Charter and Union data protection law.⁸⁰⁵ It also called on the Commission “to pursue a consistent and effective approach regarding the transfer of PNR data to third countries for the purpose of combating terrorism and serious crime, building on the ICAO SARPs, and in line with the relevant requirements established under Union law”.⁸⁰⁶

⁷⁹⁸ CJEU. *Opinion 1/15 of the Court (Grand Chamber)*, ECLI:EU:C:2017:592.

⁷⁹⁹ European Commission. *Communication from the Commission to the European Parliament and the Council – The external dimension of the EU policy on Passenger Name Records*, Ref. Ares(2020)3918953. P. 1.

⁸⁰⁰ European Commission. (27 September 2019). *Security Union: The Commission recommends opening negotiations with Japan on the transfer of Passenger Name Record (PNR) data*. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5872.

⁸⁰¹ European Council. (18 February 2020). *EU-Japan PNR agreement: Council authorizes opening of negotiations*. <https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations>.

⁸⁰² Council of the EU. (24 August 2018). *Council Decision (EU) 2018/1197 of 26 June 2018 on the signing, on behalf of the European Union, and provisional application of the Strategic Partnership Agreement between the European Union and its Member States, of the one part, and Japan, of the other part*, ST/8461/2018/INIT, OJ L 216, 1–3.

⁸⁰³ European Commission. *Communication from the Commission to the European Parliament and the Council – The external dimension of the EU policy on Passenger Name Records*, Ref. Ares(2020)3918953. P. 1.

⁸⁰⁴ Council of the EU. (10 December 2019). *Council Decision (EU) 2019/2107 of 28 November 2019 on the position to be taken on behalf of the European Union within the Council of the International Civil Aviation Organization as regards the revision of Chapter 9 of Annex 9 (Facilitation) to the Convention on International Civil Aviation in respect of standards and recommended practices on passenger name record data*, OJ L 318, 117–122, P. 121–122.

⁸⁰⁵ Council of the EU. (12 May 2021), ST 8635/21. Para. 7.

⁸⁰⁶ Council of the EU. (12 May 2021), ST 8635/21. Para. 20.

4.3. TTIP & CETA Agreements

The objective of the free flow of data for the purpose of elimination of trade barriers has played a key role in international trade negotiations for years, which lead inter alia to the proposals for a “Transatlantic Trade and Investment Partnership” (TTIP)⁸⁰⁷ with the US and a proposal for a “Comprehensive Economic Trade Agreement” (CETA)⁸⁰⁸ with Canada.

Both agreements were not negotiated according to the principle of a positive list but with negative lists, which means that TTIP and CETA apply to all areas of life which are not expressly excluded. Both could therefore also affect the right to data protection of individuals. Both were negotiated as international agreements of the EU, so they could not be terminated unilaterally for any Contracting State.

Even after a negotiation period on TTIP of over three years, there was not a consolidated result in any of the nearly thirty areas of negotiation. After negotiations texts had been only available in so-called “reading rooms” and only for parliamentarians who are not allowed to speak about it, the Commission made good on its promise of greater transparency in the negotiations and published the texts on 14 July 2016. Criticism on TTIP was backed up by the Parliament in its resolution, wherein it demanded that “the EU’s *acquis* on data privacy is not compromised through the liberalization of data flows, in particular in the area of E-Commerce and financial services, while recognizing the relevance of data flows as a backbone of transatlantic trade and the digital economy⁸⁰⁹”. The European Commission wanted to have a TTIP agreement with the US concluded during the Obama administration. But there was little movement in 15 negotiating sessions. Negotiations even came to a standstill since Donald Trump, who was critical of TTIP during his election campaign, was elected POTUS.

Art. 13.5 of CETA stipulates that it should be allowed to financial institutions and transborder financial service suppliers to transfer their customers’ personal data abroad if such transfers are “in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated”. CETA applied that laws of the State of the data exporter to the data transfer, although the service as such could be directed to the EU, which could apply their own data protection laws to the same situation under the market principle. Article 20.36 regulated the enforcement of intellectual property rights. It was the main point of criticism from a data protection perspective because it would have allowed that in the course of a claim to produce information against the alleged infringer “authorities shall have the authority, upon a justified request of the right holder, to order the infringer or the alleged infringer, to provide to the right holder or to the judicial authorities, at least for the purpose of collecting evidence, relevant information as provided for in its applicable laws and regulations that the infringer or alleged infringer possesses or controls”. Since Canada, as a member of the “Five Eyes”⁸¹⁰, was involved in the NSA affair revealed by Edward

⁸⁰⁷ European Commission. (14 July 2016). *EU negotiating texts in TTIP*. <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1230>.

⁸⁰⁸ European Commission. *Proposal for a Council Decision on the signing on behalf of the European Union of the Comprehensive Economic and Trade Agreement between Canada of the one part, and the European Union and its Member States, of the other part*, COM(2016)444, (5 July 2016).

⁸⁰⁹ European Parliament. *Resolution of 8 July 2015 containing the European Parliament’s recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP)*, (2014/2228(INI)), P8 TA(2015)0252. Para. 2.(b)(xii), P. 9.

⁸¹⁰ “Five Eyes” is an intelligence alliance that includes Australia, Canada, New Zealand, the United Kingdom, and the United States. These countries are contracting Parties to the UK-USA multilateral agreement, a treaty on joint signal intelligence cooperation.

Snowden, the personal data transferred could not be protected equally from secret services and the CETA provision could therefore be contradictory to the EU level of data protection. Before signing CETA, there was therefore a lot of opposition. In Germany, for example, an initiative was launched which filed a civil action against CETA at the Federal Constitutional Court. On 13 October 2016, the German Federal Constitutional Court declined urgent appeals from one political party and several citizens' initiatives to stop the approval.⁸¹¹ He ruled that the German federal government must ensure that certain conditions are met; Germany shall therefore make a binding declaration at the time of signing that Germany assumes a unilateral right to terminate the contract. In addition, the Federal Government must ensure that only parts of the agreement which fall within the competence of the EU are applied. Finally, the judges demanded that the German CETA committee is bound to the German Parliament for the interpretation of CETA. On 30 October 2016, CETA was signed at the EU-Canada Summit in Brussels. On 15 February 2017, the European Parliament approved CETA. Provisional application applies only to those areas that are indisputably within the exclusive competence of the EU.⁸¹² Because CETA is a mixed agreement, all EU Member States must ratify it before it can fully enter into force, what has not yet happened.

4.4. Umbrella Agreement

While the Commission's decisions on Privacy Shield and Safe Harbor – annulled by the CJEU – regulated the traffic of commercial data between companies, the “Umbrella Agreement” of 2 December 2016 is a framework agreement that aims to ensure that personal data are protected when transferred by law enforcement authorities.⁸¹³ Agreements of such type usually describe a joint consent that explicitly articulates a framework of rules and principles that guides future agreements. By negotiating those, the EU and the US tried to balance the need for certainty with the need to remain sufficiently flexible to embrace new or emerging opportunities in a certain field of regulation. The Umbrella Agreement wants to “ensure a high level of protection of personal information and enhance cooperation between the United States and the European Union and its Member States, in relation to the prevention, investigation, detection or prosecution of criminal offences, including terrorism.”, Art. 1(1) Umbrella Agreement. It is closely related to the US Judicial Redress Act of 2015 (JR Act)⁸¹⁴, and “will be signed and formally concluded only after the US Judicial Redress Bill, granting judicial redress rights to EU citizens”.⁸¹⁵

There were concerns regarding the level of data protection in the Umbrella Agreement. The EU Commission stated in this respect: “At the moment, if an EU citizens' data is transferred to US law enforcement authorities and if their data is incorrect or unlawfully processed, EU citizens – non-resident in the US – are unable to obtain redress in US courts (unlike US citizens, who could ask for redress in European courts).”⁸¹⁶ The legal service of the Parliament resumed that the “EU-US Umbrella Agreement is not

⁸¹¹ German Federal Constitutional Court (BVerfG). Judgment of the Second Senate of 13 October 2016, 2 BvR 1368/16, Paras. 1–73.

⁸¹² European Commission. *Notice concerning the provisional application of the Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union and its Member States, of the other part*, OJ L 238/9. (16 September 2017).

⁸¹³ European Commission. *Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences*, OJ L 336, 3–13, (10 December 2016).

⁸¹⁴ USA. *Judicial Redress Act of 2015*, H.R. 1428 (114th), (24 February 2016).

⁸¹⁵ European Commission. (8 September 2015). *Questions and Answers on the EU-US data protection “Umbrella agreement”*. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5612.

⁸¹⁶ European Commission. (8 September 2015). *Questions and Answers on the EU-US data protection “Umbrella agreement”*. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5612.

compatible with primary EU law and the respect for fundamental rights”⁸¹⁷. In a letter to the House Judiciary Committee, The “Electronic Privacy Information Center” (EPIC)⁸¹⁸ also recommended changes to the JR Act to provide meaningful protections for personal data from non-US persons.⁸¹⁹ On 5 February 2019, as a reaction to Cloud Act and E-Evidence Regulation, the Commission adopted two recommendations for Council Decisions.⁸²⁰ Shortly after, the EDPS welcomed “that the Recommendation [to authorize the opening of negotiations in view of an international agreement between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matter] already includes important data protection safeguards, including the need to make the Umbrella Agreement applicable by reference, and supports the need for certain additional safeguards as proposed by the Commission”⁸²¹. The EDPS recalled that, in its Opinion 1/2016⁸²², it recommended essential improvements and insisted on the need to reinforce several safeguards. A new agreement between the US and the EU should not weaken those safeguards set out by the EDPS, it should increase the level of data protection by considering the specifics and risks involved for the rights and freedoms of data subjects. One approach to this could be bilateral EU-US negotiations, which are supposed to bridge the gap between Cloud Act and E-Evidence Regulation. A press release stated that the agreement with the US must be compatible with the E-Evidence Regulation.⁸²³ The European Parliament has not yet determined a negotiation position for this, though.

Despite this criticism, the Parliament gave its consent on 1 December 2016 to the conclusion of the Umbrella Agreement by the Council, which adopted its authorizing decision the day after.⁸²⁴ Since the process was then finalized for the EU, the agreement

⁸¹⁷ European Parliament, *Legal Service, Opinion of 14 January 2016*, SJ-0784/15, (14 January 2016). P. 11. This finding was based on two reasons:

- “Article 5 (3) of the Umbrella Agreement will serve as a form of “adequacy” decision, given that it will override any requirement, set out in secondary Union legislation (such as the proposed data protection package [GDPR and Directive 2016]) for the Commission to issue an adequacy decision before transfers from the EU to the US, in the field covered by the EU-US Umbrella agreement, can be considered lawful. However, the legal effects of such an adequacy decision contained in an international agreement will be significantly different to those of an adequacy decision to be adopted by the Commission under a power conferred on it by the EU legislature in secondary Union legislation. In particular, the powers of judicial review of the CJEU are very limited with respect to international agreements, when compared to the full powers the CJEU to review adequacy decisions adopted by the Commission under secondary Union legislation.”

- “The total absence of any rights of judicial redress for a data subject compromises the very “essence” of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. As a result, it is simply not possible to reach a finding that a third country offers an level of protection of personal data in respect of transfers to a third country, by competent authorities in the EU, of personal data of certain individuals covered by EU law, where that third country affords absolutely no means of judicial redress to those same individuals whose personal data is to be transferred.”

⁸¹⁸ EPIC is an independent, non-profit research organization in Washington D.C., that frequently advises Congress and the courts about emerging privacy and civil liberties issues.

⁸¹⁹ EPIC. (16 September 2015). *Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015*. <https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf>.

⁸²⁰ European Commission. *Recommendation for a Council Decision authorizing the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, COM(2019) 70 final, (5 February 2019). // European Commission. *Recommendation for a Council Decision authorizing the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185)*, COM(2019) 71 final, (5 February 2019).

⁸²¹ EDPS. (2 April 2019). *Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence*, Opinion 2/2019, https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf. P. 3.

⁸²² EDPS. (12 February 2016). *Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, Opinion 1/2016. https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf.

⁸²³ Council of the EU. (6 June 2019). *Council gives mandate to Commission to negotiate international agreements on e-evidence in criminal matters*. <https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters>.

⁸²⁴ European Parliament. *Legislative resolution of 1 December 2016 on the draft Council decision on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal*

was able to enter in force once the US authorities had completed their internal procedures, including the necessary designations under the JR Act. These had been fulfilled by the JR Act of 2015 on 26 January 2017, thus the Umbrella Agreement was able to enter into force on 1 February 2017.⁸²⁵

The Umbrella Agreement as such does not constitute the legal basis for the transfer of personal data but such basis must be found in existing agreements between the EU and the US, or in bilateral agreements between the Member States and the US, or national laws that provide for the exchange of personal data.⁸²⁶ This legal basis could be a MLAT from 2003 between the EU and the US, which entered into force on 1 February 2010.⁸²⁷ On the other hand, as the Commission also confirmed, such legal basis could also be the EU-US PNR Agreement and the EU-US TFTP Agreement⁸²⁸.

The Umbrella Agreement relates to TFPD between authorities, regardless of the nationality or residence of the data subject. It does not apply to “transfers or other forms of cooperation between the authorities of the Member States and of the United States other than those referred to in Article 2(5), responsible for safeguarding national security”, Art. 3(2). TFPD between private legal entities and the subsequent access in the US to these personal data by a US law enforcement agency or US national security agency are also not covered by the agreement. It is also stated that each Party must implement the provisions of this Agreement without arbitrary or unjustified discrimination between its own nationals and those of the other Party. This is to ensure that EU and US citizens in the application of the Agreement are treated equally, in particular when exercising their rights to access, rectification and legal remedies.

The Umbrella Agreement contains provisions that set out some data protection principles. The transfer of personal data must only take place within the scope of the Umbrella Agreement, further processing of personal data must not go beyond the purpose of the transfer and must be relevant to and not excessive in relation to the purposes of such processing. This is to ensure that transferred data are only processed in connection with prevention, investigation, detection, or prosecution of criminal offences, including terrorism. The purpose limitation can be specified by the authority through an individual case-related requirement for the processing of personal data. The specified purposes for which personal data are processed must be set forth in agreements on the TFPD other than in relation to specific cases, investigations, or prosecutions. Regarding onward transfers, this Agreement follows the consent solution. Personal data may only be forwarded to third countries or international institutions by the receiving authority if the issuing authority has expressly agreed to this beforehand. When

offences, 2016/0126(NLE), (1 December 2016). // Council of the EU. (10 December 2016). *Council Decision (EU) 2016/2220 of 2 December 2016 on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences*, OJ L 336, 1–2.

⁸²⁵ USA. Attorney General Order No. 3824-2017, *Judicial Redress Act of 2015*, 82 Fed. Reg. 7860, (23 January 2017).

⁸²⁶ European Commission. *Commission statement regarding the EU/US Agreement on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses (“Umbrella Agreement”)*, OJ L 25, (31 January 2017). P. 2: “The Commission recalls that the Umbrella Agreement does not constitute a legal basis for the transfer of personal data between the EU and the US for the prevention, investigation, detection or prosecution of criminal offences, including terrorism (see Article 1(3) of the Agreement). Rather, in combination with the applicable legal basis for the transfer and subject to the conditions set forth in Article 5 of the Agreement, the Agreement aims to provide appropriate safeguards within the meaning of Article 37(1) of Directive 2016/680 [LED]. By contrast, the Agreement does not provide a general authorization for transfers. Furthermore, the Agreement preserves the ability of national data protection authorities to fully exercise their supervisory powers granted by EU law as regards international transfers falling within its scope.”

⁸²⁷ EU. *Agreement on mutual legal assistance between the European Union and the United States of America*, OJ L 181, 34–40, (19 July 2003).

⁸²⁸ European Commission. *Commission statement regarding the EU/US Agreement on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses (“Umbrella Agreement”)*, OJ L 25, (31 January 2017).

granting this consent, the initiating authority “shall take due account of all relevant factors, including the seriousness of the offence, the purpose for which the data is initially transferred and whether the State not bound by the present Agreement or international body in question ensures an appropriate level of protection of personal information”, Art. 7(2). An onward transfer “may only take place in accordance with specific conditions set forth in the agreement that provide due justification for the onward transfer. The agreement shall also provide for appropriate information mechanisms between the Competent Authorities”, Art. 7(3). The issuing authority cannot deny its consent or impose conditions based on the level of data protection in the State or the body of the receiving Party. In special agreements that allow the transfer of large amounts of personal data (Big Data), the standards and conditions that are relevant for these processings must be specified in more detail; this applies in particular regarding the processing of sensitive data, onward transfers, and storage periods. If a data breach is discovered, the receiving authority must notify the issuing authority. The Agreement introduces retention and storage periods to ensure that data are only stored for as long as necessary. When determining these periods, the purpose of the collection and processing, the type of data, the processing body and the effects on the data subject and other applicable legal considerations should be considered.

The Agreement also regulates the rights of data subjects, which are information, access, correction, deletion, as well as an administrative and a judicial remedy. The data subject, whose personal data are transferred, is granted a subjective right to authorization and access regarding its personal data; the data subject can contact the receiving – designated – agency in the country of destination to execute these rights. The other requirements of the right to correction are to be based on the local law of the receiving authority. If a data breach is discovered, the receiving authority must notify the issuing authority. It is also provided that the person concerned must be notified. Judicial redress is governed by Art. 19. “In line with this provision, the US adopted the Judicial Redress Act that extended important judicial redress provisions of the US Privacy Act to EU citizens, including in relation to Passenger Name Record (PNR) and Terrorist Finance Tracking Program (TFTP) data”, commented the Commission as an answer to a question by a Member of the European Parliament.⁸²⁹ As authorities can restrict these data subject rights, for example for reasons of national security, MEP Sophie in ‘t Veld questioned “the effective enactment by the U.S of their obligations as per the EU-US Umbrella Agreement”⁸³⁰.

There is no information available if the first joint review of the Umbrella Agreement, which was scheduled for 1 February 2020, has been concluded. On 8 December 2020, the Commissioner commented on MEP Sophie in ‘t Veld’s request as follows:

As required by Article 23 of the Umbrella Agreement, the effectiveness of such redress mechanisms is one of the main issues to be assessed by the ongoing review. This will also be addressed in the Commission’s report. Following the annulment of the Privacy Shield, there is willingness between the Commission and the US authorities to work together to find ways by which to address the issues raised by the Court of Justice of the EU.⁸³¹

⁸²⁹ European Commission. (8 December 2020). *Answer given by Mr Reynders on behalf of the European Commission, E-004472/2020*. https://www.europarl.europa.eu/doceo/document/E-9-2020-004472-ASW_EN.pdf.

⁸³⁰ in ‘t Veld, Sophie. (26 January 2017). *Letter to EU Commission: What impact has Trump decisions on Privacy Shield and Umbrella Agreement?*. <https://www.sophieintveld.eu/letter-to-eu-commission-what-impact-has-trump-decisions-on-privacy-shield-and-umbrella-agreement>.

⁸³¹ European Commission. (8 December 2020). *Answer given by Mr Reynders on behalf of the European Commission, E-004472/2020*. https://www.europarl.europa.eu/doceo/document/E-9-2020-004472-ASW_EN.pdf.

It remains thus be seen whether the data subject rights guaranteed in the Umbrella Agreement will be deemed to be in fact appropriately “implemented”, or findings made that e.g., the right to notification is significantly delayed in practice due to the wide interpretation of the concept of national security prevailing in the US.

4.5. Horizontal provisions

The Commission saw the need to explore “synergies between trade and data protection instruments [...] to ensure free and safe international data flows that are essential for the business operations, competitiveness and growth of European companies, including SMEs, in the increasingly digitalized economy”⁸³² and was “determined to tackle digital protectionism”.⁸³³ The Commission would like to remedy data flow restrictions⁸³⁴ through “horizontal provisions that rule out such unjustified restrictions”⁸³⁵.

Those “horizontal provisions” in future EU trade agreements are aimed at ensuring TFPD to facilitate trade in the digital economy. However, there is always the field of tension that Naef has analyzed: “The architecture of EU law gives primacy to fundamental rights over international law. The EU thus cannot negotiate data flow clauses in trade agreements that compromise its high data protection standards.”⁸³⁶

To remedy these threats for a free TFPD while preserving the regulatory autonomy of the Parties to protect the fundamental right to data protection, the EU “developed specific provisions on data flows and data protection in trade agreements which it systematically tables in its bilateral – most recently with Australia, New Zealand, and the UK – and multilateral negotiations such as the current WTO E-Commerce talks”⁸³⁷. It has also “intensified its dialogue in a number of bilateral, regional and multilateral fora”⁸³⁸, including meetings of the G20 and G7 groups, which “have also recently recognized the contribution of data protection to trust in the digital economy and data flows, in particular through the concept of Data Free Flow with Trust originally proposed by the Japanese G20 Presidency”⁸³⁹. At the last meeting of the G7, TFPD were again discussed. The prospect was raised to “create options for businesses to choose cross-border transfer tools, suitable for their business needs”. The conclusions after this meeting also annotated that the goal should be “to gradually align the regulators’ approaches to privacy and better understand domestic rules in each jurisdiction” and found that countries “need legislation guaranteeing that individuals’ personal data is only accessed if strictly necessary for national security purposes”.

⁸³² European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 13.

⁸³³ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 12.

⁸³⁴ See Chapter VIII, Section I.

⁸³⁵ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 13.

⁸³⁶ Naef, T. [Tobias]. *Data Protection without Data Protectionism*. Springer. P. 425.

⁸³⁷ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 13.

⁸³⁸ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 12.

⁸³⁹ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 12.

III. Legislation of the Council of Europe

1. European Convention on Human Rights

Driven and supported by civil society actors, a European movement (more than 700 citizens from 16 European countries), started at the Hague Congress in 1948, designed a European human rights charter and called for their monitoring by European courts. This movement contributed decisively to the establishment of the CoE in 1949 and the ECHR, which entered into force on 3 September 1953.

From the perspective of international law, provisions of the ECHR are in principle binding on all Contracting Parties that have ratified it and for which it has entered into force. Isolated exceptions exist for reservations (Art. 57 ECHR), emergency situations (Art. 15 ECHR) or after termination of accession (Art. 58 ECHR). Those Parties signed the convention at that time: Belgium, Denmark, France, Germany, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Turkey, and the United Kingdom. The ECHR can only be signed by members of the CoE and by the EU.⁸⁴⁰ 47 States have ratified the convention. Russia has been excluded from the ECHR due to the war in Ukraine, and “six months after its exclusion from the Council of Europe, the Russian Federation ceases to be party to the European Convention on Human Rights on 16 September 2022. The European Court of Human Rights remains competent to deal with applications against Russia concerning actions or omissions occurring up until 16 September 2022.”⁸⁴¹

The ECHR is a multilateral international agreement in favor of third Parties and the commitments for the Parties are intended to offer benefit to all people who are subject to the sovereign power of the Parties. According to Art. 1 ECHR, the Parties guarantee the rights and freedoms to the persons under their jurisdiction. The entitled persons must be able to exercise fundamental rights and be in a relationship with the State bound by the ECHR. The territorial scope covers the territory of each Party. The temporal scope of application extends from the entry into force of the ECHR for the Party concerned until its withdrawal from the CoE.

Alike the UN Charter, the Statute of the CoE focuses on peacekeeping, international cooperation, and the protection of fundamental rights.⁸⁴² The Statute of the CoE provides for the rule of law principle in Art. 3. It also underlines that the protection of human rights for the CoE is not just one of several objectives, but its “*Raison d’Être*” (reason to be). The CoE’s regulatory policy program on human rights protection reflects the values of democratic societies. Nevertheless, the reach of the provisions does not go beyond the UN human rights program. The CoE’s human rights standards have been formulated more precisely so that the States concerned can rely less on exceptions to restrict rights. The most important difference between the CoE and the UN systems is not the different interpretations of substantive norms but the institutionalization of procedures for implementing the norms.

The monitoring of compliance with the conventions in the European human rights system is based on three procedures alike those in the UN system: the reporting obligation, the State complaint, and the individual complaint. Within the framework of the ECHR, the

⁸⁴⁰ CoE. (29 September 2020). *The EU’s accession to the European Convention on Human Rights*. <http://www.coe.int/en/web/portal/-/the-eu-s-accession-to-the-european-convention-on-human-rights>.

⁸⁴¹ CoE. (16 September 2022). *Russia ceases to be party to the European Convention on Human Rights*. <https://www.coe.int/en/web/portal/-/russia-ceases-to-be-party-to-the-european-convention-on-human-rights>.

⁸⁴² CoE. *Statute of the Council of Europe*, ETS No. 001, (5 May 1949). Art. 1(1).

Secretary-General may invite Member States to report on the implementation of their obligations under the ECHR. The “weakest” form of control is, as in the UN system, the reporting obligation. According to Art. 8 of the Statute of the CoE, a serious violation of these obligations may lead to the Party being suspended from its rights of representation and requested by the Committee of Ministers to withdraw from the Convention, Art. 46(2) ECHR.

According to Art. 46(1) ECHR, the Parties are obliged to comply with judgments of the ECtHR. Since the entry into force of the 11th Additional Protocol, the jurisdiction of the ECtHR has no longer been subject to a separate declaration of subjection by the Contracting Parties to the ECHR but is compulsory of its own.⁸⁴³ Since then, the ECtHR has been the sole decision-making body as a permanent court, Art. 19 ECHR. The extent to which judgments issued against other States can also have binding legal effects is still disputed, the prevailing opinion assumes only an *inter partes* effect under Art. 46 ECHR.⁸⁴⁴ Since no Party’s measure can be annulled or amended by a judgment of the ECtHR itself, the monitoring of human rights practice can only work if the members of the CoE themselves voluntarily submit to the ECtHR’s judgments. Otherwise, the CoE has only a few sanction options available, which go beyond the public denunciations of the respective Party. If the ECtHR finds in its judgment a violation of the ECHR, it urges this Party to take measures to avoid comparable human rights violations in the future and may notify this Party to change its laws and administrative acts, Art. 1 ECHR. In addition, this Party may be sentenced for compensation, Art. 41 ECHR. The implementation of these measures is monitored by the Committee of Ministers. To this end, the Committee receives reports by this Party on the implementation of the measures imposed.

The ECHR encompasses the protection of four rights: “Everyone has the right to respect for his private and family life, his home and his correspondence.”⁸⁴⁵ The provision is similar to Art. 17 of the “International Covenant on Civil and Political Rights” (ICCPR)⁸⁴⁶, whereby the latter adds honor and reputation as protected assets. The wording of Art. 8 ECHR opens a space for interpretation of the scope of protection. According to Art. 32(1) ECHR, the interpretation of the ECHR, including its protocols, is the responsibility of the ECtHR. The Court has hereby to respect the principles of treaty interpretation, which rely upon the VCLT. This means that the ICCPR, signed by all Parties to the CoE, can be also used as an interpretive source of international law applicable to Parties to the ECHR. The ECtHR can therefore also use the practice of the UN HRC on Art. 17 ICCPR for the interpretation of Art. 8 ECHR and hereby contribute to the coordination between human rights protection at European as well as global level.

The ECtHR found in several judgments that Art. 8 ECHR also encompasses data protection.⁸⁴⁷ The processing of personal data is included in the scope of protection. However, the Court recalled the necessary connection of these data to “private life”, thus to the narrower *ratio legis* of Art. 8 ECHR.⁸⁴⁸ The mere existence of personal data (which does not necessarily have to relate to the private sphere)⁸⁴⁹ might therefore not be

⁸⁴³ CoE. *Protocol No. 11 to the Convention for the protection of human rights and fundamental freedoms, restructuring the control machinery established thereby*, ETS 155, (11 May 1994).

⁸⁴⁴ See for example Grabenwarter, C. [Christoph]. (2010). Wirkungen eines Urteils des Europäischen Gerichtshofs für Menschenrechte – am Beispiel des Falls M. gegen Deutschland, *Juristenzeitung* 65(18), 857–869. P. 859.

⁸⁴⁵ Art. 8(1) ECHR

⁸⁴⁶ UN, Office of the High Commissioner for Human Rights. *International Covenant on Civil and Political Rights*, General Assembly resolution 2200A (XXI), (16 December 1966).

⁸⁴⁷ E.g., ECtHR, Judgment of 19 September 2013, *von Hannover v Germany*, Application no. 8772/10. Para. 41. // ECtHR, Judgment of 4 December 2008, *S. u. Marper v UK*, Application no. 30562/04. Para. 103

⁸⁴⁸ ECtHR, Judgment of 17 February 2011, *Wasmuth v Germany*, Application no. 12884/03. Para. 74. // ECtHR, Judgment of 26 March 1987, *Leander v Sweden*, Application no. 9248/81. Para. 48.

⁸⁴⁹ See also Chapter I, Section II.5.1.

sufficient. Protection in scope may be the case for data which are of personal nature and have a sufficient relevance to personality. Protection is therefore guaranteed for special categories of data, such as personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life. Art. 8 ECHR can preclude the collection and storage of data.⁸⁵⁰ The monitoring of a public square in the opinion of the ECtHR does not infringe private life, but the creation of stored images of surveillance does.⁸⁵¹ The creation of movement profiles through GPS surveillance is also regarded as being in scope of Art. 8 ECHR.⁸⁵² The retention of data is also an interference with the rights protected by Art. 8 ECHR; if such data collections serve the purpose of a Member State's intelligence services, an interference is only justified if necessary and only if certain guarantees against misuse are provided and taken into account.⁸⁵³ Domestic law must therefore provide sufficient guarantees against data misuse; the Party's authorities have a margin of discretion when it comes to balancing interests.⁸⁵⁴

Interference with the rights protected by Art. 8 ECHR can also consist of omitting action because the ECHR also includes a positive obligation for a Party.⁸⁵⁵ In its defensive function, Art. 8 ECHR is intended to prevent interference by measures of a Party. Such interference can result in a claim by affected individuals for the omission of unlawful interference and, in addition, a claim for the elimination of reversible interferences. These aspects are considered when examining whether a Party has exceeded its discretion in assessing proportionality of an interference. In individual cases, a Party must also enact efficient laws that prevent serious crimes against the values protected in Art. 8 ECHR, especially where essential values of private life are affected. It must also ensure that rules are enforced through effective investigations and criminal proceedings in the event of an interference. Art. 8 ECHR may result in the obligation to enforce respect for private and family life in the private sphere as well. The positive obligation can also include measures in the relationship between private individuals.⁸⁵⁶ It is challenging to precisely delimit the negative obligation to cease and desist from the positive obligation to act. In both cases, a fair balance must be struck between the conflicting interests of the individual and the community.

The legitimacy of the interference requires that, derived from the rule of law principle of the ECHR, that interference must be suitable, necessary, and appropriate, and the law which allows for an interference must be precise. The ECtHR, particularly in cases of interferences which are not recognizable to the data subjects, attaches importance to the assessment of the appropriateness of the interference. The ECtHR also noted that the right to the protection of personal data cannot be guaranteed without limitation but must also be reconciled with the rights of others.⁸⁵⁷ Moreover, the provision that allows

⁸⁵⁰ ECtHR, Judgment of 26 March 1987, *Leander v Sweden*, Application no. 9248/81. Para. 48.

⁸⁵¹ ECtHR, Judgment of 28 January 2003, *Peck v United Kingdom*, Application no. 44647/98. Para. 59.

⁸⁵² ECtHR, Judgment of 2 September 2010, *Uzun v Germany*, Application no. 35623/05. Para. 49ff.

⁸⁵³ ECtHR, Judgment of 6 September 1978, *Klass et al v. Germany*, Application no. 5029/71. Para. 49. // ECtHR, Judgment of 13 November 2012, *M.M. v the United Kingdom*, Application no. 24029/07. Para. 199.

⁸⁵⁴ ECtHR, Judgment of 25 February 1997, *Z. v Finland*, Application no. 22009/93. Paras. 95ff. // ECtHR, Judgment of 4 December 2008, *S. u. Marper v UK*, Application no. 30562/04. Para. 103.

⁸⁵⁵ ECtHR. *Guide on Article 8 of the European Convention on Human Rights*,

https://www.echr.coe.int/documents/guide_art_8_eng.pdf, (31 August 2022). P. 8–10. // Provisions similar to Art. 1(1) ECHR can be found in Art. 1(1) of the American Convention on Human Rights (Inter-American Specialized Conference on Human Rights. *American Convention on human rights*, (22 November 1969)), and in relation to the African Charter on Human and Peoples' Rights (African Commission on Human and Peoples' Rights. *African Charter on Human and Peoples' Rights*, (27 June 1981)) through an interpretation by the *Commission Nationale Des Droits De l'Homme Et Des Liberté v. Chad*, Communication 4/92, 9th ACHPR AAR Annex VIII (1995-1996), which found that "States Parties shall not only recognize the rights duties and freedoms adopted by the Charter, but they should also "undertake [...] measures to give effect to them".

⁸⁵⁶ ECtHR, Judgment of 12 June 2003, *van Kück v. Germany*, Application no. 35968/97. Para. 70

⁸⁵⁷ ECtHR. *Guide on Article 8 of the European Convention on Human Rights*,
https://www.echr.coe.int/documents/guide_art_8_eng.pdf, (31 August 2022). P. 7.

interferences must be sufficiently clear and precise.⁸⁵⁸ The ECtHR also noted that “the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained”.⁸⁵⁹

While public denunciation by the CoE does not necessarily lead to changed human rights practices in the respective Member States of the ECHR, the position of the ECtHR gives the human rights norms of the European framework a considerable effectiveness. The frequent appeal to the ECtHR may be an indication of the acceptance of the EHCR. Every individual can lodge a complaint against alleged human rights violations directly before the ECtHR, Art. 34 ECHR. Like any ordinary court, the ECtHR must then independently examine the complaint. The total number of complaints raised with an annual rate of 40.600 in 2015, 53.500 in 2016, 53.300 in 2017, 56.350 in 2018, 59.800 in 2019, 61.500 in 2020, 70,150 in 2022, and 74.650 as of 5 May 2023; State complaints account for a small percentage of this.⁸⁶⁰

However, the efficiency of the ECHR is threatened by some aspects: Before a complaint to the ECtHR, the recourse to national courts must be exhausted before an individual can turn to the ECtHR.

The ECHR is a “security network” if the primarily responsible human rights protection system fails in a Member State of the ECHR. The ECHR offers supranational human rights protection against State acts, but not against acts of the CoE. Although the pending cases reduced through the so-called *Interlaken* process,⁸⁶¹ the workload of the Court is still extensive, and the complaints can only be examined with significant delay. As noted by Kinsch

the duration of the proceedings before the ECtHR is still too long in the vast majority of cases. This is actually paradoxical: the guarantee enshrined in Art 6(1) ECHR that a judicial decision will be delivered ‘within a reasonable time’ cannot be applied to these proceedings themselves. Periods of five years or more are not uncommon in those cases that actually lead to a judgment.⁸⁶²

The procedure of the individual complaint is lengthy. It may take up to one year or more before the ECtHR can begin the examination; the procedure in the Court usually takes five to seven years.⁸⁶³ The enlargement of the Parties from originally 10 to today 47 States has further aggravated this situation. The relationship between the CJEU and the

⁸⁵⁸ ECtHR, Judgment of 4 December 2008, *S. u. Marper v UK*, Application no. 30562/04. Paras. 95ff.

⁸⁵⁹ ECtHR, Judgment of 4 December 2008, *S. u. Marper v UK*, Application no. 30562/04. P. 67.

⁸⁶⁰ CoE. (January 2016). *Analysis of statistics 2015*. http://www.echr.coe.int/Documents/Stats_analysis_2015_ENG.pdf. // CoE. (January 2017). *Analysis of statistics 2016*. http://www.echr.coe.int/Documents/Stats_analysis_2016_ENG.pdf. // CoE. (January 2023). *Analysis of statistics 2022*. https://www.echr.coe.int/Documents/Stats_analysis_2022_ENG.pdf. // Legal Tribune Online. (29 January 2020). *Wir werden weitere Gutachten-Verfahren sehen*. <https://www.lto.de/recht/justiz/j/egmr-jahresbericht-statistik-2019-beschwerden-russland-tuerkei-gutachten-verfahren>. // Statista GmbH. (31 May 2021). *Anzahl der anhängigen Verfahren am Europäischen Gerichtshof für Menschenrechte nach beklagten Ländern*. <https://de.statista.com/statistik/daten/studie/76450/umfrage/anhaengige-verfahren-am-europaeischen-gerichtshof-fuer-menschenrechte>.

⁸⁶¹ ECtHR, (1 June 2016). *The Interlaken process and the Court (2016 Report)*. https://www.echr.coe.int/Documents/2016_Interlaken_Process_ENG.pdf https://www.echr.coe.int/Documents/2016_Interlaken_Process_ENG.pdf. // CoE. (June 2020). *Supervision of the execution of judgements and decisions of the European Court of Human Rights 2019 - 13th Annual Report of the Committee of Ministers (2020)*. <https://edoc.coe.int/fr/convention-europenne-des-droits-de-l-homme/8176-supervision-of-the-execution-of-judgements-of-the-european-court-of-human-rights-2018-12th-annual-report-of-the-committee-of-ministers.html>. P. 51.

⁸⁶² Kinsch, P. [Patrick]. (2009). *European Court of Human Rights (ECtHR)*. [https://max-eup2012.mpipriv.de/index.php/European_Court_of_Human_Rights_\(ECtHR\)](https://max-eup2012.mpipriv.de/index.php/European_Court_of_Human_Rights_(ECtHR)).

⁸⁶³ CoE. (June 2020). *Supervision of the execution of judgements and decisions of the European Court of Human Rights 2019 - 13th Annual Report of the Committee of Ministers (2020)*. <https://edoc.coe.int/fr/convention-europenne-des-droits-de-l-homme/8176-supervision-of-the-execution-of-judgements-of-the-european-court-of-human-rights-2018-12th-annual-report-of-the-committee-of-ministers.html>. P. 73.

ECtHR is consolidated but not conclusively clarified, particularly due to the unclear prospect of EU accession to the ECHR. In terms of procedural law, there has so far been no connection between the CJEU and the ECHR. As the EU has not yet joined the ECHR, the Union is formally not subject to the jurisdiction of the ECHR; a complaint to the ECtHR against decisions of the CJEU or other acts of the Union is therefore not possible. In the case law of the ECHR, however, there is the possibility of indirect control over Union actions via a control of actions by Union Member States, which are indeed subject to the ECHR (Art. 1 ECHR). Until now, major interpretation differences have been avoided by mutual consideration of the jurisprudence in both courts. However, this “dialogue” of the courts is increasingly endangered, as the binding nature of the Charter leads to a strengthening of the CJEU in questions of fundamental rights and an increase in competence in this area. The worst-case scenario is that in the future there will be two sets of case law on the same fundamental rights; this would not help to promote the legal certainty in Europe and could have a negative effect on a congruent interpretation of privacy-related norms in the European framework.

2. Convention on Cyber Crime

The “Convention on Cybercrime of the Council of Europe” (CCC), also known as the “Budapest Convention” has been ratified by 68 States, among them almost all CoE Member States (except Ireland and Russia) and several non-European countries, including the US, Chile, Ghana or Japan, which makes the Convention a global standard for the fight against cybercrime.⁸⁶⁴ It was the first international agreement in this regulatory area, which, in addition to tools for international cooperation, contains a catalog of norms for harmonizing national rules. The CCC is supplemented by the first additional protocol to the Convention to regulate access to electronic evidence on servers “in the cloud”.⁸⁶⁵ The “Second Additional Protocol” has been adopted on 12 May 2022.⁸⁶⁶

At European level, before the LED, there was no legal act that regulated the collection of electronic evidence and particularly its data protection requirements. Directive 95/46 and E-Privacy Directive excluded the applicability to criminal proceedings, the Data Retention Directive 2006/24/EC was annulled by the CJEU in 2014 and the Framework Decision 2008/977/JHA was suspended by the LED.

The main objective of the CCC, set out in the Preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The Parties undertake to incorporate several criminal offenses (Arts. 2–12 CCC) against computers and with the help of computers into their national substantive law, to give their law enforcement authorities additional powers to secure – subject to the rule of law guarantees (Art. 15 CCC) – electronic evidence (Arts. 16–21 CCC), and to cooperate with other Parties (Arts. 23–35 CCC). The provisions are not limited to computer crime but are applicable to all criminal offenses for which evidence is found on computers (Art. 14 CCC).

The provisions of the CCC address both domestic and transborder access to data. They serve as a guideline for countries to develop national legislation against Cybercrime and as a framework for international cooperation between the Parties. The CCC deals with crime committed on the Internet and other computer networks. It obliges the contracting

⁸⁶⁴ CoE. *Convention on Cybercrime*, ETS No. 185, (1 July 2004).

⁸⁶⁵ CoE. *Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems*, ETS No. 189, ETS No. 189, (1 March 2006).

⁸⁶⁶ CoE. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, CETS No. 224, (12 May 2022).

Parties to determine powers and procedures to obtain electronic evidence and to provide mutual legal assistance. The Parties are required to issue production orders to collect data from SPs on their territory or from SPs which offer their services to a Party's territory. These data – subscriber-, traffic- or content data – can then be requested via a MLAT (Art. 31 CCC). In addition, the Convention provides for preservation orders if there is reason to believe that the data are particularly at risk of loss or change, Art. 29 CCC. A simplified procedure and a 24/7 network are provided under Art. 35 CCC (so-called “quick freeze”).

Direct access to foreign servers (so-called “transborder search”) generally requires authorization under international law because it affects foreign territory, where it triggers data processing activities, which can affect national criminal law and/or national data protection law. The most specific rule of the CCC on Tbfd – Art. 32 CCC – regulates the access to data abroad without the involvement of the authorities of this target country, which allows direct access to all freely accessible information on the Internet (lit. a) and to data voluntarily made available by the data subject (lit. b). The problem with Art. 32(b) CCC is that direct access could undermine a basic principle of international legal cooperation, namely that of dual criminality. The same applies to the possibility of refusing cooperation, if this affects the sovereignty, security, public order, or other essential interests of the Party. In addition, the protection of the individual granted by criminal law or data protection law could be impaired or transborder access could affect the rights of third Parties, for example those of a SP. In practice, obtaining the lawful consent of the data subject could be problematic, because a SP cannot be the one who voluntarily enables access to data.⁸⁶⁷ In addition, the law enforcement authorities must be sure that the server in question lies in a Party's territory. However, it is often unclear what importance the seat of the provider, the location of the server, or the location of personal data have in the internal policy of a provider, and to which Contracting Party investigating authorities should therefore be directed. In practice, States and law enforcement agencies could therefore develop their own national solutions for a transborder access to data. The “Transborder Group” established

that an additional protocol on transborder access to data would be needed, but that such a Protocol is controversial in the current context.⁸⁶⁸ [...] The Transborder Group believes that in the absence of an international framework with safeguards, countries will take unilateral action and extend law enforcement powers to remote transborder searches either formally or informally with unclear safeguards. Such unilateral assertions of jurisdiction will not be a satisfactory solution.⁸⁶⁹

The current debate under the CCC aims at a contractual agreement on enhanced transborder investigative powers.⁸⁷⁰ The search for an international framework for transborder access to data with the necessary “safeguards” also played a role when the Second Additional Protocol to the CCC had been negotiated since February 2019. The Second Additional Protocol “provides a legal basis for disclosure of domain name registration information and for direct co-operation with SPs for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection

⁸⁶⁷ CoE. *Transborder access to data and jurisdiction: Options for further action by the T-C, T-CY* (2014)16, (3 December 2014). P. 11.

⁸⁶⁸ CoE. *Transborder access to data and jurisdiction: Options for further action by the T-C, T-CY* (2014)16, (3 December 2014). P. 12.

⁸⁶⁹ CoE. *Transborder access to data and jurisdiction: Options for further action by the T-C, T-CY* (2014)16, (3 December 2014). P. 13.

⁸⁷⁰ European Commission. (5 February 2019). *Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention*. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_865.

safeguards.”⁸⁷¹ With the new legal basis, law enforcement authorities can now request subscriber-, traffic-, as well as – in “emergencies” – content data. The latter may involve a situation where there is a significant and imminent risk to the life or safety of a natural person. As examples, the text of the Second Additional Protocol mentions “immediate aftermath of a terrorist attack, a ransomware attack that may cripple a hospital system, or when investigating e-mail accounts used by kidnappers to issue demands and communicate with the victim’s family”⁸⁷². The Parties may also request content data in a non-urgent case, but in doing so they must use other (such as bilateral) MLAT procedures.⁸⁷³

3. Convention 108 / Convention 108+

Convention 108 was agreed by the Member States of the CoE on 28 January 1981 and entered into force on 1 October 1985. As of 26 June 2023, 55 States ratified Convention 108.⁸⁷⁴ With Convention 108, the Parties wanted to ensure data protection within the system of the CoE by requiring the Parties to protect the fundamental rights of the individuals living in their territory against the automated processing of personal data and to allow the free TFPD to other signatory countries. The aim was to concretize and implement the protection of private life guaranteed by Art. 8 ECHR.⁸⁷⁵

Convention 108 emerged ten years before the “Guidelines for the Regulation of Computerized Personal Data Files” (UN Guidelines)⁸⁷⁶ and one year after the OECD Guidelines 1980. When drafting Convention 108, the OECD had already set out a similar task with the OECD Guidelines 1980, but more from a trade- than human rights perspective⁸⁷⁷. Nevertheless, both OECD Guidelines 1980 and Convention 108 had similarities in many aspects due to the “extensive co-operation that took place between the bodies charged with drafting the two codes”⁸⁷⁸.

In 1999, an amendment of Convention 108 was made allowing the European Communities and International organizations to accede, Arts. 27 and 28 Convention 108.⁸⁷⁹ In 2001, the CoE enacted the Additional Protocol⁸⁸⁰, which entered into force on 1 July 2004. Regarding its purpose, the CoE stated:

With the increase in exchanges of personal data across national borders, it is necessary to ensure the effective protection of human rights and fundamental freedoms, and in particular the right to privacy in relation to such exchanges of personal data. The Protocol requires Parties to set up supervisory authorities, exercising their functions in

⁸⁷¹ CoE. (17 November 2021). *Cybercrime: Council of Europe strengthens its legal arsenal*.

https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a48ca6.

⁸⁷² CoE. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Explanatory Report*, CM(2021)57-addfinal, (17 November 2021). Para. 148.

⁸⁷³ CoE. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Explanatory Report*, CM(2021)57-addfinal, (17 November 2021). Para. 70.

⁸⁷⁴ CoE. (24 June 2023). *Chart of signatures and ratifications of Treaty 108*. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.

⁸⁷⁵ Preamble of Convention 108

⁸⁷⁶ UN, General Assembly. *Guidelines for the Regulation of Computerized Personal Data Files*, Resolution 45/95, (14 December 1990).

⁸⁷⁷ See also Chapter IX, Section III.1.1.

⁸⁷⁸ Bygrave, L. A. [Lee A.]. (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar. P. 27.

⁸⁷⁹ CoE. *Amendments approved by the Committee of Ministers, in Strasbourg, on 15 June 1999*, <https://rm.coe.int/168008c2b8>, (15 June 1999).

⁸⁸⁰ CoE. *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*, ETS No. 181, <https://rm.coe.int/1680080626>, (8 November 2001).

complete independence, which are an element of the effective protection of individuals with regard to the processing of personal data.⁸⁸¹

Art. 12(2) Convention 108 guarantees a free flow of personal data between Parties to this Convention but neither provides nor requires restrictions on onward TFPD to States that are not Parties to Convention 108. Therefore, once a non-European State becomes Party to Convention 108, it is not necessarily obliged to have a data export restriction provision in its law, but such provision needs to be in place when acceding to the Additional Protocol. Similarly to the provisions in Directive 95/46 (therein Arts. 25ff.), Parties to the Additional Protocol have to legislate that personal data may only be disclosed to a recipient who is under the jurisdiction of a non-Party to Convention 108, if this non-Party can ensure an adequate level of protection; exceptions to this requirement were permitted within narrow limits. Just as the Convention 108 itself, the Additional Protocol established no rights for individuals, but merely obliged the Parties to legislate. The absence of jurisdictional rules for TFPD was a major shortcoming of Convention 108. A further amendment to the Convention 108 was therefore suggested and the “Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (T-PD) encouraged to start preparing a second additional protocol of Convention 108.⁸⁸² The 30th Council of Europe Conferences of Ministers of Justice also expressed its support for an amendment of Convention 108 in Resolution 3.⁸⁸³

Since then, a process included opinions and proposals from various stakeholders. Two bodies of the CoE were responsible for the modernization of Convention 108. T-PD was established based on Art. 20(4) Convention 108 and is made up of representatives of all CoE Member States. T-PD exercises the attributions provided by Arts. 19 and 20 of Convention 108. It issues draft legal instruments in view of their adoption by the Committee of Ministers and also opinions and reports. The Committee has a Bureau (T-PD-BUR) in charge of the preparation of the reunions of the T-PD. But

T-PD only represents the Parties to the Convention and is composed of national experts belonging to independent supervisory authorities in certain cases and from governments in others (for instance Ministries of Justice, Interior, Telecommunication). A number of questions raised during the modernization exercise, such as the strengthening of the follow-up and evaluation mechanism and the corresponding role of the Committee of the Parties, need to be discussed at inter-governmental level involving all 47 Member States. Enabling Member States and other Parties to the Convention to appoint governmental representatives with specific subject-matter expertise is essential.⁸⁸⁴

Therefore, CAHDATA was established⁸⁸⁵ “to provide a high-level inter-governmental forum for negotiation, to ensure consistency and complementarity with the relevant European Union’s framework as well as to support the global potential of Convention 108”⁸⁸⁶. During summer 2016, CAHDATA and T-PD discussed the influences to be considered for a future content of a new version of Convention 108, which led in September 2016 to the issuing of the updated working document as “Draft modernized

⁸⁸¹ CoE. (2023). *Convention 108 and Protocols*. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.

⁸⁸² CoE. *20th meeting of the Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, T-PD-BUR (2010) RAP 20, (16 March 2010).

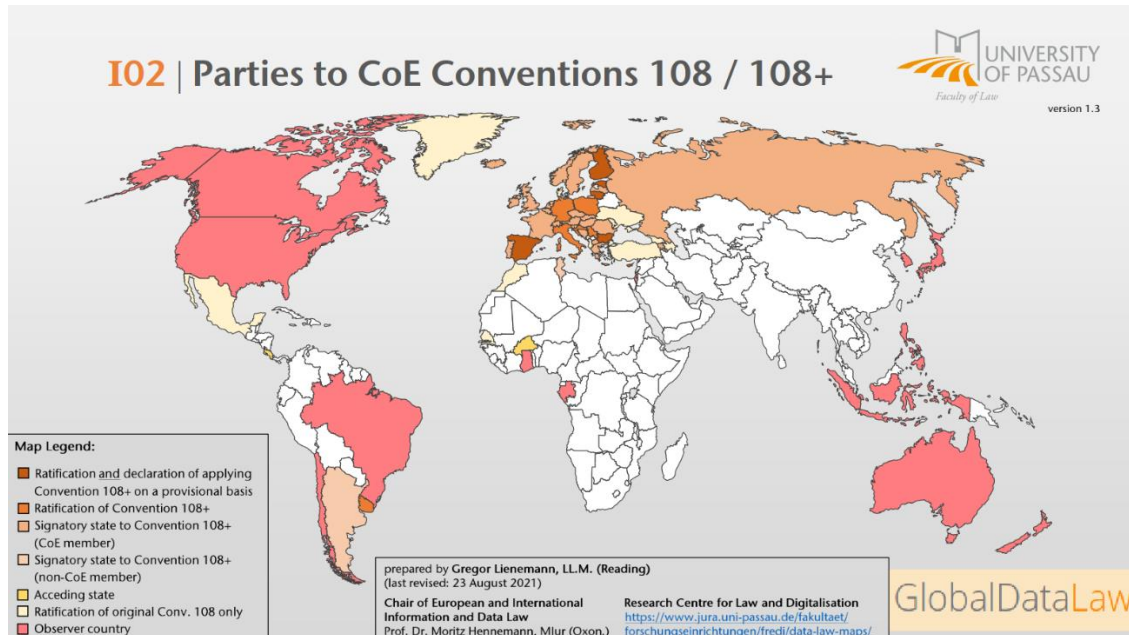
⁸⁸³ CoE. *Resolution No. 3 on data protection and privacy in the third millennium*, MJU-30 (2010) RESOL. 3, (26 November 2010).

⁸⁸⁴ CoE. *Information Document*, CAHDATA(2013) Inf, (17 September 2013). P. 4.

⁸⁸⁵ CoE. *Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods*, (9 November 2011). Art. 17.

⁸⁸⁶ CoE. *Information Document*, CAHDATA(2013) Inf, (17 September 2013). P. 4.

Convention for the Protection of Individuals with Regard to the Processing of Personal Data”⁸⁸⁷ and the “Draft explanatory report to the Convention 108 modernized”⁸⁸⁸. At the 128th Session of the Committee of Ministers, Convention 108+ was adopted and has been open for signature since 10 October 2018,⁸⁸⁹ together with an Explanatory Report⁸⁹⁰. On As of 24 June 2023, 26 countries have ratified Convention 108+,⁸⁹¹ which means an increase of 13 Parties to Convention 108+ within about 2 years.



Source: Lienemann, G. [Georg], “Parties to CoE Conventions 108 / 108+ (23 August 2021)”⁸⁹²

It should be borne in mind that entry into force of Convention 108+ can only occur upon ratification by all Parties to the Additional Protocol, or as of 11 October 2023, once 38 Parties to the Convention have ratified the First Protocol.

Convention 108+ contains the following improvements:

- Higher requirements regarding the principles of proportionality and data minimization as well as the lawfulness of processing;
- Extension of the categories of sensitive data, which now also include genetic and biometric data as well as data regarding union membership and ethnic origin;
- Obligation to report data protection violations;
- Greater transparency of data processing;
- New rights for data subjects in connection with algorithmic decision-making processes

⁸⁸⁷ CoE. *Draft modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, GR-J(2016)1, (September 2016).

⁸⁸⁸ CoE. *Draft explanatory report – Convention 108 modernized*, <https://rm.coe.int/16806b6ec2>, (24 August 2016).

⁸⁸⁹ CoE. *128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018)*, *Ad hoc Committee on Data Protection (CAHDATA) – Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, CM(2018)2-final, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e, (18 May 2018).

⁸⁹⁰ CoE. *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS No. 223, (10 October 2018). (“Explanatory Report to Convention 108+”).

⁸⁹¹ CoE. (23 June 2023). *Chart of signatures and ratifications of Treaty 223*. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures>.

⁸⁹² Lienemann, G. [Georg]. (23 August 2021). *Parties to CoE Conventions 108 / 108+*. https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/lehrstuehle/hennemann/Mapping_Global_Data_Law/Sample_Conventi_on_108.pdf

- Strengthened accountability of those responsible for data processing;
- Requirement that the “Privacy by Design” principle is applied;
- Clear regime of TFPD
- Strengthened powers and independence of SAs and legal basis for international cooperation.

The legal definitions in Art. 2 Convention 108+ largely coincide with the GDPR, the Charter, and the OECD Guidelines 1980. Convention 108+ applies to the processing of personal data in the public and private sectors, Art. 3(1) Convention 108+. In Convention 108, Art. 3(2)(a) still provided for the possibility that States would not apply the Convention to certain types of personal data. On this basis, some States had, for example, declared not to apply Convention 108 to data processing activities carried out by public bodies for the purposes of national security, defense, and the investigation and prevention of crime. This possibility of not applying Convention 108+ to certain areas no longer exists in the 2018 version. Data processing carried out by an individual in the course of purely personal or household activities is excluded from scope, Art. 3(2) Convention 108+. Geographically, Convention 108+ extends to Member States of the CoE, but also Non-Members of the CoE can accede.

Convention 108+ imposes binding obligations under international law. Nevertheless, a recourse to the ECtHR must be based on an alleged violation of the ECHR and not Convention 108+.

Art. 14(1) Convention 108+ contains in its first sentence the principle for a free TFPD.⁸⁹³ A Party may invoke two exceptions from this principle. Besides those two exceptions, Convention 108+ “does not restrict the freedom of a Party to limit the transfer of personal data to another Party for other purposes, including for instance national security, defense, public safety, or other important public interests (including protection of state secrecy)”.⁸⁹⁴ The notion of “national security” should be interpreted based on the relevant case law of the ECtHR.⁸⁹⁵

The first exception applies, “if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention”. The exception must be interpreted restrictively, a Party cannot rely on it in cases where the risk is either hypothetical or minor.⁸⁹⁶ It should therefore only apply, if the Party

has clear and reliable evidence that transferring the data to another Party could significantly undermine the protections afforded to that data under the Convention, and that the likelihood of this happening is high. This might be the case, for instance, when certain protections afforded under the Convention are no longer guaranteed by the other Party (for instance because its supervisory authority is no longer able to effectively exercise its functions) or when data transferred to another Party is likely to be further transferred (onward transfer) without an appropriate level of protection being ensured.⁸⁹⁷

⁸⁹³ “A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorization the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so if bound by harmonized rules of protection shared by States belonging to a regional international organization.”

⁸⁹⁴ Explanatory Report to Convention 108+. Para. 105.

⁸⁹⁵ Explanatory Report to Convention 108+. Para. 96.

⁸⁹⁶ Explanatory Report to Convention 108+. Para. 106.

⁸⁹⁷ Explanatory Report to Convention 108+. Para. 106.

It is questionable whether “having clear and reliable evidence” indicates an interpretation in a sense of an “obligation” for the Party to assess the legal framework in the recipient country. The Explanatory Report to Convention 108+ states that the “level of protection should be assessed for each transfer or category of transfers”, which indeed indicates such obligation for the data exporter to conduct a GDPR-like assessment before the data transfer.⁸⁹⁸ Interestingly, the second sentence of Art. 14(1) Convention 108+ uses the expression “may prohibit or subject to special authorization”, which looks to be contrary to the “prohibition principle” in Art. 6(1) GDPR and reads like a “permit with ban reservation”.

The second exception set out in the third sentence of Art. 14(1) Convention 108+ applies

where Parties are bound by harmonized rules of protection shared by States belonging to regional (economic) organizations that seek a deeper level of integration. Among others, this applies to the member states of the EU. However, as explicitly stated in the General Data Protection Regulation (EU) 2016/679, a third country’s accession to Convention 108 and its implementation will be an important factor when applying the EU’s international transfer regime, in particular when assessing whether the third country offers an adequate level of protection (which in turn allows the free flow of personal data).⁸⁹⁹

This indicates that in the case of undergoing a TIA under Art. 46(2)(c) GDPR, it is necessary to consider whether the recipient State is a Party to Convention 108+.

Art. 14(2) Convention 108+ ensures that data processed by a recipient within the jurisdiction of a Party remains protected by appropriate data protection principles, even if the recipient of the personal data in the jurisdiction of a Party carries out an onward transfer of these data to a recipient in the jurisdiction of a non-Party. Art. 14(2) Convention 108+ applies only to the outflow of data from the jurisdiction of a Party to such of a non-Party, not to its inflow between Parties’ jurisdictions since the latter scenario is already covered by the data protection regime of the recipient Party. “Appropriate data protection” is to be interpreted in a way that “protection afforded has to be of such quality as to ensure that human rights are not affected by globalization and transborder data flows.”⁹⁰⁰ However,

Parties may transfer data even in the absence of an appropriate level of protection where this is justified, among others, by prevailing legitimate interests, in particular important public interests to the extent these are provided for by law and such transfers constitute a necessary and proportionate measure in a democratic society (*littera c.*). Personal data may thus be transferred on grounds that are similar to those listed in Article 11, paragraphs 1 and 3.⁹⁰¹

Measures to ensure that level can be “the law of that State or international organization, including the applicable international treaties or agreements; or ad hoc or approved standardized safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing” (Arts. 14(3)(a) and Art. 14(3)(b) Convention 108+). These Articles “apply to all forms of appropriate protection, whether provided by law or by standardized safeguards”⁹⁰². This

⁸⁹⁸ Explanatory Report to Convention 108+. Para. 110.

⁸⁹⁹ Explanatory Report to Convention 108+. Paras. 106–107.

⁹⁰⁰ Explanatory Report to Convention 108+. Para. 103.

⁹⁰¹ Explanatory Report to Convention 108+. Para. 108.

⁹⁰² Explanatory Report to Convention 108+. Para. 110.

protection must include the “relevant elements of data protection”⁹⁰³ and the appropriateness

should be assessed for each transfer or category of transfers. Various elements of the transfer should be examined, such as: the type of data; the purposes and duration of processing for which the data are transferred; the respect of the rule of law by the country of final destination; the general and sectoral legal rules applicable in the State or organization in question; and the professional and security rules which apply there.⁹⁰⁴

These enforceable instruments can be contractual clauses or binding corporate rules which must also be “duly implemented”.⁹⁰⁵

On 3 March 2023, the T-PD released a revised version of the draft “Model Contractual Clauses for the Transfer of Personal Data from Controller to Controller” (CoE MCC) under Convention 108+;⁹⁰⁶ “these Clauses, together with their Annexes which form an integral part thereof provide an appropriate level of protection for the transfer of Personal data within the meaning of Article 14(2), (3)(b) of the Convention”⁹⁰⁷. The CoE MCC largely follow the structure of the SPDC. They “include new definitions, including for the terms ‘data breach’, ‘data exporter’, and ‘data importer’, and amend existing clauses, such as those on: due diligence and cooperation between the data importer and the data exporter; data security; onward transfers; and redress for data subjects”.⁹⁰⁸ They

also offer the possibility to make certain choices, the so-called “options”, and require signatories to include details of the data transfers and security measures in the annexes. However, some differences remain. Unlike the EU SCCs [SDPC], which consist of four different modules, the CoE MCCs are limited to one scenario for both controllers and processors. Additionally, while the EU SCCs are a standardized tool for data transfers in all EU member states, Convention 108+ parties may decide whether or not to approve the CoE MCCs as their standardized tool. Finally, although the general structure of the EU SCCs and the CoE MCCs is similar, the obligations do not fully overlap. For example, both sets of clauses envisage data breach reporting but differ in the reporting modalities. The revised CoE MCCs are still a work in progress, and the final version may turn out to be more or less like the EU SCCs [SDPC].⁹⁰⁹

Even in the absence of an appropriate level of protection, a Party may provide that the transfer of personal data may take place if the data subject “has given specific and free consent, after being informed of risks arising in the absence of appropriate safeguards” (Art. 14(4)(a) Convention 108+), “the specific interests of the data subject require it in the particular case” (Art. 14(4)(b) Convention 108+), “prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society” (Art. 14(4)(c) Convention 108+) or “it constitutes a necessary and proportionate measure in a democratic society for freedom of expression” (Art. 14(4)(d) Convention 108+). The reference to “measure in a democratic society” is equivalent to the provisions of the

⁹⁰³ Explanatory Report to Convention 108+. Paras. 110–111.

⁹⁰⁴ Explanatory Report to Convention 108+. Para. 110.

⁹⁰⁵ CoE. *The modernized Convention 108: novelties in a nutshell*. <http://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8>. P. 5.

⁹⁰⁶ CoE. *Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, Model Contractual Clauses for the Transfer of Personal Data*, T-PD(2022)1rev8, (3 March 2023). (“CoE MCC”).

⁹⁰⁷ MCC. Art. 1(1).

⁹⁰⁸ OneTrust. (7 March 2023). *International: CoE issues revised draft model contractual clauses*.

<https://www.dataguidance.com/news/international-coe-issues-revised-draft-model>.

⁹⁰⁹ IAPP. (June 2023). *A practical comparison of the EU, China and ASEAN standard contractual clauses*.

<https://iapp.org/resources/article/a-practical-comparison-of-the-eu-china-and-asean-standard-contractual-clauses/#sccs>.

GDPR, the LED, the ECHR and the *Schrems* judgments. The legitimacy of exceptions is then subject to a necessity and proportionality test. In this case, the need for a measure is not addressed in a uniform way but must be determined considering the realities of the domestic law of that Party. In the cases of Arts. 14(3)(b) and 14(4)(b)–(c) Convention 108+, Arts. 15(5)–(6) Convention 108+ regulate obligations to ensure that all relevant information is made available to the competent SA within the meaning of Art. 15 Convention 108+ and, in order to demonstrate the effectiveness of the safeguards or the existence of overriding legitimate interests, to the SA.

Art. 18 Convention 108+ grants persons resident abroad the right to assistance from the State of their residency in the exercise of their national rights. Authorities may only reject the request from the authority of another Member State as well as an application for assistance by a person living abroad under to specific conditions specified in Art. 16 Convention 108+. Art. 23 Convention 108+ provides for the possibility of the accession of non-Member States of the CoE under certain conditions. This provision shows that Convention 108+ is designed as a treaty with potentially global scope. In accordance with Art. 29 Convention 108+, reservations are not permitted. However, Convention 108+ may be terminated under Art. 30 Convention 108+ at any time. Cancellation shall take effect on the first day of the month, following a period of six months after the notification is received by the CoE Secretary General.

CHAPTER III: US FRAMEWORK

A TFPD to and from the US is of particular importance in practice. The US “has adopted a number of laws that restrict what private sector actors in specific sectors are permitted to do with personal data they collect, in particular with respect to finance, healthcare, students and under-aged persons. Similar laws have been enacted at the state level in many parts of the USA, leading to a colorful, if confusing, picture of privacy law in the United States”⁹¹⁰.

I. Jurisprudence and variations of the right to privacy

The Fourth Amendment prohibits indiscriminate searches of place, person, instruments, and property and requires the request for a “search warrant”⁹¹¹ based on a reasonable suspicion.⁹¹² However, the term “search” has never been interpreted by the Supreme Court as an “act of searching for or in something”, but rather oriented itself towards its interpretation on the right to property as well as the principles of privacy. The scope of application of the Fourth Amendment was thus restrictive. The Supreme Court further interpreted the use of the “search” regarding property interests. According to this, a “search” only existed if a public authority had any kind of unauthorized access to property rights. For this reason, the interception of telephones was not considered a “search”, since interception by tapping telephone lines outside of a house was possible. However, the listening by means of a board bug mounted on the skirting did indeed cover the scope of protection of the Fourth Amendment. However, this property-based interpretation was reinterpreted in relation to privacy. In the decision *Katz v. US*, the Supreme Court made a traditional property-oriented interpretation of the term “search” but added that “what [a person] seeks to preserve as private, even in an area accessible to the public” is a constitutionally protected area.⁹¹³ This case introduced the “Katz test” to determine a reasonable expectation of privacy in a so-called “two-stage test”. A reasonable expectation thus exists if the person concerned had a particular privacy expectation (stage 1) and this expectation was also objectively recognized by the society (stage 2).⁹¹⁴ In Supreme Court decisions after *Katz v. US*, the scope of protection of the Fourth Amendment had been further adjusted. According to the so-called “plain view rule” or “open field doctrine”,⁹¹⁵ there can be no justified privacy expectation if a place is openly visible.

Katz v. US left unprotected anything a person knowingly exposes to the public, which led to the decision *US v. Miller*, and developed the so-called “third party doctrine”. This doctrine contains that people who voluntarily give information to third Parties have “no

⁹¹⁰ Chase P. [Peter] et al. (July 2016). *Transatlantic digital economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU%282016%29535006_EN.pdf. P. 23.

⁹¹¹ Government agencies requiring communications providers to disclose electronic communications content, Section 2703(a) of the SCA.

⁹¹² “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

⁹¹³ USA. *Katz v. United States*, Supreme Court, 389 U.S. 347, (1967).

⁹¹⁴ Schwartz, P. [Paul] and Solove, D. [Daniel]. (2021). *Information Privacy Law*. Wolters Kluwer. P. 300.

⁹¹⁵ First introduced in US Supreme Court. *Hester v. United States*, 265 U.S. 57, (1924).

reasonable expectation of privacy”.⁹¹⁶ In *US v. Miller* it was found that customer data stored by a bank are not covered by the scope of the Fourth Amendment, if these data are transmitted to government agencies, because a customer who discloses his personal data to a third party (his bank) consents to a transfer to public authorities.⁹¹⁷ This applies even if data are onwarded, expecting that the data would only be used in accordance with a contract.⁹¹⁸ This was affirmed by the decision of *Smith v. Maryland*⁹¹⁹, finding that a customer of a telephone company has no reasonable privacy expectations for the processing of his chosen telephone numbers, as he has voluntarily provided the data to the service provider.⁹²⁰ The consequence of these decisions were that the Fourth Amendment offered no protection in cases where personal data were obtained from a data subject for public authorities whilst the subject knows or should know that the third Party processes the data. The Supreme Court hereby upheld the third-party doctrine developed in *US v. Miller*. The Court found that the Fourth Amendment is not implicated if the government sought access to these data. This exclusion of data disclosed to third Parties meant that all data are available to the government without constitutional limit, which posed risks to individuals’ fundamental rights in times of US surveillance actions justified with a “significant purpose”, being foreign intelligence measures.

In US literature, there are several statements that illustrate the confusion in making “privacy” understandable and tangible. Judith Jarvis Thomas stated: “Perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is.”⁹²¹ McCarthy compared the concept of privacy with that of the freedom and States: “Like the emotive word freedom, privacy means so many different things that so many different people that it has lost any precise legal connotation that it might have had.”⁹²² Solove said: “It seems as though everybody is talking about ‘privacy’, but it is not clear exactly what they are talking about” and that “Privacy, therefore, consists of many different yet related things.”⁹²³ In addition to these still more neutral opinions on the complexity of privacy, there were also some negative views. For example, Fred Cate said that privacy is “an antisocial construct [...] [that] conflicts with other important values within the society, such as society’s interest in facilitating free expression, punitive crime, private property, and conducting government operations efficiently.”⁹²⁴ Privacy should therefore also be understood as what it appears to be, that means complex but containing different manifestations of its sense. Some concepts of how privacy is understood are to be examined in the following.

Common law as the basis of US laws traditionally did not know a right to privacy and granted only limited protection of fundamental rights. At first it only applied to the area of honor protection under the term “defamation”, to which tort (written defamatory statements) and slander (verbal defamatory statements) belonged. The first initiative to make this protection more comprehensive was based on Warren / Brandeis. Their article “The right to privacy”, often regarded as the foundation of Privacy Law in the US, was published in the *Harvard Law Review* in 1890.⁹²⁵ They referred to a comment by Judge Thomas Cooley on the law of torts of 1880, in which he used the expression “the right to be let alone” to explain that attempted physical touching could be qualified as a tortious

⁹¹⁶ USA. *United States v. Miller*, Supreme Court, 425 U.S. 435, (1976).

⁹¹⁷ USA. *United States v. Miller*, Supreme Court, 425 U.S. 435, (1976). P. 443.

⁹¹⁸ USA. *United States v. Miller*, Supreme Court, 425 U.S. 435, (1976). P. 443.

⁹¹⁹ USA. *Smith v. Maryland*, Supreme Court, 442 U.S. 735, (1979).

⁹²⁰ USA. *Smith v. Maryland*, Supreme Court, 442 U.S. 735, (1979). P. 743.

⁹²¹ Jarvis Thomson, J. [Judith]. (1975). The Right to Privacy. *Philosophy & Public Affairs*, 4(4), 295–314- P 295.

⁹²² McCarthy, T. [Thomas]. (1999). *The rights of publicity and privacy*. Clark Boardman Callaghan. Para. 5.59.

⁹²³ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. P. 5, 9, 42 ff.

⁹²⁴ Cate, F. [Fred]. (1997). *Privacy in the information age*. Brookings Institution Press. P. 30.

⁹²⁵ Brandeis, L. [Louis] and Warren, S. [Samuel]. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220.

act, but still does not define a right to privacy.⁹²⁶ In the following, Warren / Brandeis used this term to show that a right to privacy is implicitly anchored in common law.⁹²⁷ The article by Warren / Brandeis may be interpreted as a reaction to the practice of the “gossip-press” that was published at the time, which was a constant source of revelations from celebrity life. Warren / Brandeis analyzed English and American judgments, each of which, in favor of the plaintiffs, with the help of common law institutes, established an interference with privacy.⁹²⁸ The result of this analysis was that all decisions were taken based on a right to privacy and that common law actually acknowledges this right.

The article “Privacy” by William L. Prosser in 1960 also influenced this development.⁹²⁹ An estimate that Prosser made regarding the importance of the essay by Warren / Brandeis can now also be applied to his own essay: “It has come to be regarded as the outstanding example of the influence of legal periodicals upon American law”.⁹³⁰ Prosser distinguished four torts of infringements of personality rights according to the relevant case law; these torts were:

1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.⁹³¹

These allowed to claim certain infringements of fundamental rights, though the scope of application remained limited. He compared these with four corresponding claims for tortious justice, which had gained consistent recognition in US case law and US legislation, and in so-called “Restatements of the Law”⁹³² of the American Law Institute.

Despite the importance of the essay by Warren / Brandeis for tort- and case law, and the discussion of privacy in the US in general, “the right to be let alone” as an understanding of privacy was sometimes considered too far and too unshapely tailored for situations in which one should be left alone. However, the importance of “the right to be let alone” as an attempt to explain what is meant by privacy in the US should be noted.

Privacy in the US is also understood as “limited access to the self”, as the missing ability to protect oneself from unwanted intrusion by others, and thus as a concept that complements the concept of “right to be let alone”; this concept includes, inter alia, freedom from public interference, from the press and others, and acknowledges that privacy goes beyond a mere isolation from others, and it thus encompasses not only the deliberate withdrawal, but also the intervention from outside.⁹³³ There is a multitude of different forms of this category. For example, it is defined as “[...] the access to others - either physical access, personal information, or attention”⁹³⁴ or “[...] a degree of inaccessibility is an important necessary condition for the apt application of privacy”⁹³⁵.

⁹²⁶ Brandeis, L. [Louis] and Warren, S. [Samuel]. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220. P. 195.

⁹²⁷ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. P. 16.

⁹²⁸ Brandeis, L. [Louis] and Warren, S. [Samuel]. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220. P. 193 ff.

⁹²⁹ Prosser, W. [William]. (1960). Privacy. *California Law Review*, 48(3), 383–423.

⁹³⁰ Prosser, W. [William]. (1960). Privacy. *California Law Review*, 48(3), 383–423. P. 383.

⁹³¹ Prosser, W. [William]. (1960). Privacy. *California Law Review*, 48(3), 383–423. P. 389.

⁹³² Restatements exist for all areas of law, often already in second or third review, and systematically record case law in the external form of a European legal textbook. These usually help to get a quick overview of the legal situation regarding a specific question. They are not authoritative but reach such a level of reliability in their review of the relevant case law that lawyers and courts use to cite those.

⁹³³ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. P. 16.

⁹³⁴ Bok, S. [Sissela]. (1982). *Secrets: On the Ethics of Concealment and Revelation*. Pantheon Books. P. 10-11.

⁹³⁵ Allen, A. [Anita]. (1988). *Uneasy access*. Rowman & Littlefield. P. 10.

Another category is “secrecy”, which means that privacy is violated when previously secret information is publicly disclosed. For example, privacy was described as “an outcome of a person’s wish to share with others certain knowledge as well as its past and present experience and action and its intentions for the future”⁹³⁶. In US case law, privacy is sometimes understood in accordance with the concept of “secrecy” as the limitation of a disclosure of secret information. The US Supreme Court in *Whalen v. Roe* ruled that the constitution protects a so-called “zone of privacy”, which includes not only “independence in the making of certain kinds of important decisions”, but also “individual interest in avoiding disclosure of personal matters”⁹³⁷. “Secrecy” can be understood as a subcategory of the concept of “limited access to the self”, with “secrecy” being narrower as it covers only one dimension of “limited access to the self”, namely the disclosure of personal matters.

The control over personal data was considered the next category. Fried defined privacy “not simply an absence of information about us in the minds of others; rather, it is the control we have over information about ourselves”⁹³⁸. Miller found that “[...] the basic attribute of an effective right of privacy is the individual’s ability to control the circulation of information pertaining to him”.⁹³⁹ The Supreme Court also argued that privacy is the control of an individual over information pertaining to his person (“individual’s control of information concerning his or her person”).⁹⁴⁰ This category does not include aspects of privacy that are not to be understood as informational, such as the right to make certain fundamental decisions or the way in which one educates one’s children. On the other hand, the concept may well be considered too broad if the aspect of “control” is not exactly defined.⁹⁴¹

The way to protect the integrity of personality can be seen as another category. This concept is not independent of the previously presented and can be used in conjunction with these to explain the importance of privacy to decide which unwanted interventions by others are worthy of protection or what kind of information should be exercised. Jeffrey Reiman defined the right to privacy as follows: “The right to privacy [...] protects the individual’s interest in becoming, being, and remaining a person.”⁹⁴² In his reply to Prosser’s aforementioned essay, Bloustein also dealt with privacy and argued that it primarily protects individuality.⁹⁴³ There are also decisions in the Supreme Court case law which point to an understanding of privacy in relation to personality and in which, above all, the freedom of choice of the person is at the forefront. In *Planned Parenthood of Southeastern Pennsylvania et al. v. Casey*, the court understood that, for the protection of privacy, non-interference by the State in certain key decisions that define personality is essential: “These matters, including the most intimate and personal choices lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourth Amendment. At the heart of liberty is the right to define one’s own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood

⁹³⁶ Jourard, S. [Sidney]. (1966). Some Psychological Aspects of Privacy. *Law and Contemporary Problems*, 31(2), 307–318. P. 307.

⁹³⁷ USA. *Whalen v. Roe*, Supreme Court, 429 U.S. 589, (1977). P. 599–600.

⁹³⁸ Fried, C. [Charles]. (1968). Privacy. *Yale Law Journal*, 77(3), 475–493. P. 482.

⁹³⁹ Miller, A. [Arthur]. (1971). *Der Einbruch in die Privatsphäre*. Luchterhand. P. 25.

⁹⁴⁰ US Supreme Court. *United States Department of Justice v. Reporters Committee For Freedom of the Press*, 489 U.S. 749, (1989). P. 763.

⁹⁴¹ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. P. 28 f.

⁹⁴² Reiman, J. [Jeffrey]. (1984). Privacy, intimacy, and personhood. In F. D. [Ferdinand David] Schoeman, *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, (1984), 300–316. P. 314.

⁹⁴³ Bloustein, E. [Edward]. (1964). *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*. *New York University Law Review*, 39(6), 962–1007. P. 973 f., 981 f.

were they formed under compulsion of the State.”⁹⁴⁴ The court was sometimes criticized for equating privacy with freedom and, in particular, free will.⁹⁴⁵ In general, theories that primarily understood personality in private life were criticized because they lack the adequate definition of personality to clarify what privacy means and theories are often too broad, since personality does not play exclusively in the private sphere.⁹⁴⁶

The last category presented by Solove understands privacy as a form of intimacy and argues that privacy is not only essential for individual self-creation, but also for human relationships. The value of privacy lies hereby in the development of personal relationships and the category tries to define for which aspects of life the possibility of shielding should exist or in relation to which information control or secrecy is possible.⁹⁴⁷ However, the category can be seen as too broad on the one hand and too narrow on the other: Too broad if the term “intimacy” is not adequately defined, because without the appropriate restrictions, the word “intimacy” is just another word for privacy and not sufficient to determine what matters are included; and too narrow since information about one’s own financial circumstances would also be covered by privacy, but these would not be compatible with the understanding of privacy as “intimacy”.⁹⁴⁸

In *Dobbs v. Jackson Women’s Health Organization*⁹⁴⁹, the Supreme Court reversed its *Roe v. Wade*⁹⁵⁰ decision on 24 June 2022. Basically, the *Roe v. Wade* decision gave women the right to decide whether to terminate or continue a pregnancy. While this right was “fundamental,” it was not “absolute.” This may also have implications for the future scope of the right to privacy in the US. This decision stokes people’s fears that the government is

clearly eager to violate their privacy and the basic human right to control their own bodies. Besides urging U.S. Congress to work quickly to codify *Roe v. Wade*, [US Senator] Wyden said an immediate and necessary response to the decision would be to pass federal privacy legislation. Congress must pass legislation protecting people’s data so their web searches, text messages and location tracking aren’t weaponized against them, Wyden said. Technology companies must take immediate steps to limit the collection and retention of customer data so that they don’t become tools of persecution.⁹⁵¹

II. Regulatory instruments

1. Federal legislation

To put US federal law instruments in the context of the reasons for their adoption at the time, their analysis should be in the following carried out as chronological as possible. Since the 9/11 attacks, practice in the US framework led to a rising quantity of cases related to the war on terror and located US legislation increasingly between motives of the judiciary and the US “Intelligence Community” (IC) on one side and (foreign)

⁹⁴⁴ USA. *Planned Parenthood of South-eastern Pennsylvania et al. v. Casey*, Supreme Court, 505 U.S. 833, (1992). P. 851.

⁹⁴⁵ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. P. 31.

⁹⁴⁶ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. P. 31.

⁹⁴⁷ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. P. 34.

⁹⁴⁸ Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press. P. 36 f.

⁹⁴⁹ USA. *Thomas E. Dobbs, State Health Officer of the Mississippi Department of Health, et al., Petitioners v. Jackson Women’s Health Organization, et al.*, Supreme Court, No. 19–1392, (2022).

⁹⁵⁰ USA. *Roe v. Wade*, Supreme Court, No. 70-18, (1973).

⁹⁵¹ Duball, J. [Joseph]. (27 June 2022). *Roe v. Wade reversal sends ripples through privacy world*. <http://iapp.org/news/a/roe-v-wade-reversal-sends-ripples-through-privacy-world>.

fundamental rights on the other. This Section II.2.1 is therefore divided into “pre-9/11” and “post-9/11” instruments.

1.1. Pre-9/11 instruments

1.1.1. Privacy Act

The Privacy Act governs how the federal government manages personal data in its possession. The “Fair Information Practice Principles” (FIPP)⁹⁵² of the FTC concern information practice in an electronic marketplace and are reflected in the Privacy Act, but there are also a variety of exemptions and practices that dilute the scope of application.

A restriction to the flow of personal data in the international context was debated in the context of the negotiations on the Privacy Act, but ultimately not adopted. One key point of the Privacy Act discussed in the committees was that data flow should only be permitted if the data subject’s consent had previously been obtained or if the provisions of the law itself, secured by a contract of appropriate content, were complied with. The draft regulation was found both in § 201 (a) (6) of the Bill of Rights 3418 of the Privacy Act, which included the private and public sector, as well as in the revised bill 3633 in § 4 (a) (6), which had only the public sector as a regulatory subject. By requiring compliance with the provisions of the Privacy Act on the basis of a data processing contract, as an alternative to obtaining consent, the law would have required quasi-equivalence with regard to the level of protection abroad. Notably, the equivalence required went beyond the adequacy of the level of protection in the third country as required by Directive 95/46. If the proposed law would have been adopted in this proposed format, many of the EU-US data transfer problems would probably not have arisen. A regulation adopted in this form in one of the first US data protection laws would possibly also have had influenced future instruments as a model. The skeptical attitude of the private sector and the public sector regarding such a law ultimately hindered a wider consideration of TFPD.

The Privacy Act in its adopted format is “an Act to amend title 5, United States Code, by adding a Section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.”⁹⁵³ Only information that is stored in a “system of records” is in scope. This system is understood as “group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual”, § 552a (a) (5).

The Privacy Act prohibits the disclosure of personal data from a system of records without the written consent of the data subject unless this disclosure is subject to one of twelve exceptions. The law also gives individuals the ability to access and modify their records of personal data and sets out various requirements for storing such records. It guarantees three basic rights:

- The right to review those records that are kept by the government, subject to exemptions,

⁹⁵² FTC. (25 June 2009). *Fair Information Practice Principles*.

<https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm>.

⁹⁵³ Privacy Act. Preamble.

- The right to request changes to those records to ensure that they are correct, relevant, timely or complete, and
- The right to be protected from unjustified or illegal intrusions into privacy resulting from the collection, maintenance, use and disclosure of your personal data.

However, until the JR Act came into effect, only US citizens were entitled to these rights. Moreover, the Privacy Act allows federal agencies to exempt systems of records from most of the duties of the Privacy Act, e.g., for PNR data and similar law enforcement databases. This led – until the Umbrella Agreement⁹⁵⁴ (especially Art. 19 Umbrella Agreement) – to the situation that judicial redress was *de facto* not sufficiently granted to EU citizens when it came to TFPD under the EU-US PNR Agreement or the EU-US TFTP Agreement.

1.1.2. Executive Order 12333

The EO 12333, which is also referred to in the *Schrems II* judgment, allows the NSA to access data “on the way” to the US by accessing submarine cables laid on the bottom of the Atlantic, as well as collecting and storing personal data before arriving to the US and being subjected to FISA regulations.⁹⁵⁵ The CJEU concluded that US surveillance programs based on Section 702 FISA, EO 12333 and PPD-28 do not indicate that adequate protection exists for non-US persons potentially being covered by these programs. Under these circumstances, these three legal bases are not suitable for guaranteeing a level of protection that is essentially equivalent to the level guaranteed by Art 7, 8, 52 of the Charter. Therefore, an examination of these legal bases is necessary in the following.

The EO 12333 is a presidential decree of the POTUS Ronald Reagan from 4 December 1981, with which he expanded powers and responsibilities of national intelligence services. In addition, Reagan instructed the heads of the US federal authorities to cooperate with the CIA, which provided for the transfer of data. EO 12333 authorizes the collection of international intelligence information outside the US and sets principles and priorities. The minimization procedures used to limit the targeted surveillance of US persons remain secret. The relevant authorities, National Security Council (NSC) and Director of National Intelligence (DNI), are responsible for supervision. In December 2013, in the wake of the Snowden Affair, the NSA announced that this order would allow it to monitor cell phones globally.⁹⁵⁶ EO 12333 was the primary authority for surveillance measures that were not covered by the “Electronic Communications Privacy Act of 1986” (ECPA)⁹⁵⁷ or FISA; that includes most surveillance by US intelligence agencies outside the US.⁹⁵⁸ As most surveillance by US intelligence agencies was conducted outside the US, EO 12333 was the primary legal basis used for most surveillance by US intelligence agencies.⁹⁵⁹

⁹⁵⁴ See Chapter I, Section II.4.4.

⁹⁵⁵ *Schrems II*. Para. 63.

⁹⁵⁶ Sasso, B. [Brandan]. (12 June 2013). *NSA tracks phone locations under executive order*. <https://thehill.com/policy/technology/192294-nsa-uses-executive-order-to-track-phone-locations>.

⁹⁵⁷ USA. *Electronic Communications Privacy Act of 1986*, 18 U.S.C. §§ 2510–2523.

⁹⁵⁸ Electronic Frontier Foundation. (24 July 2014). *12333 flowchart*.

<http://www.eff.org/files/2014/07/24/12333flowchart.pdf>.

⁹⁵⁹ Greenwald, G. [Glenn] and MacAskill, E. [Ewan]. (11 June 2013). *Boundless Informant: the NSA's secret tool to track global surveillance data*. *The Guardian*. <https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>. // Electronic Frontier Foundation. (15 November 2013). *Memorandum OC-034-12*.

https://www.eff.org/files/2013/11/15/20130816-wapo-sid_oversight.pdf. // Gellman, B. [Barton] and Soltani, A. [Ashkan]. (4 December 2013). *NSA tracking cellphone locations worldwide, Snowden documents show*. *The Washington Post*. https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

The use of EO 12333 for national intelligence agencies procedures endangered the separation of powers in the US. The US executive branch has several powers related to national security and foreign intelligence. It is long been the understanding that the POTUS at the top of that branch has a degree of “inherent power” to conduct intelligence operations. Closer details on the reach of this power comes from “*Youngstown Sheet & Tube Co. v. Sawyer*”⁹⁶⁰, also commonly referred to as the “Steel Seizure Case”. There are three categories on executive powers set out in this judgment. The first relates to executive conduct that US Congress has previously authorized; in that category, POTUS’ “authority is at its maximum”⁹⁶¹. If some conduct is unlawful then only because the federal government entirely lacks constitutional power for that conduct. ECPA and FISA fall into that category. The second category applies when US Congress has not addressed an issue. In those areas, POTUS acts “in a zone of twilight”⁹⁶². The scope of the POTUS’ inherent power is informed by historical practice in contemporary necessities. This is the area where EO 12333 provides primary guidance. This area includes foreign intelligence operations outside the US. The third category consists of executive conduct that US Congress has forbidden. In those areas the POTUS’ “power is at its lowest ebb”⁹⁶³. In this category there is a conflict between the powers of the US Congress according to Art. 1 of the US Constitution and POTUS’ powers according to Art. 2 of the US Constitution. In the years following the 9/11 attacks, the Bush Administration engaged in surveillance practices that fell within this third category even when the Department of Justice concluded that some of the surveillance practices in place were unlawful, but others were a valid exercise of aforementioned Art. 2 powers. In the late Bush Administration this category was still used for conducts which the executive branch called “International Transit Switch Collection”, operated under “Transit Authority”, which applies to international telecommunications traffic as they traverse US territory.⁹⁶⁴

The main criticisms about EO 12333 are that there is no sufficient judicial oversight. FISA doesn’t cover these operations affecting personal data, the “Foreign Intelligence Surveillance Act Court” (FISC) is not involved. There is only little transparency by the executive branch which also led to the fact that research on the use of EO 12333 in practice comes almost exclusively from leaks. It is also theoretically possible to circumvent EO 12333 by relocating intelligence operations outside the US instead of collecting transatlantic Internet traffic in the US by partnering with foreign intelligence agencies. As it has come to the public attention, the NSA partnered for example with United Kingdom’s Government Communications Headquarters (GCHQ) und Germany’s *Bundesnachrichtendienst*. The NSA received then the exact same information but was – according to the US intelligence agencies legal theory – subject to a different set of legal protections. Finally, the same objections to FISA Section 702 can be raised for EO 12333 because foreign individuals and businesses receive little protection and US citizens are subject to massive incidental collection (“bulk collection”).

In January 2014, the POTUS Barack Obama issued PPD-28, the latest guidance for those surveillance operations, which is also to be seen in context with EO 12333. Non-US persons can therefore be targeted for surveillance without court approval. That surveillance requires only “a foreign intelligence purpose”. That is a requirement more “lax” than FISA Section 702, which requires “a significant foreign intelligence purpose”. Under the old rules before PPD-28, there were even lesser disclosure and use protections for US citizens.

⁹⁶⁰ USA. *Youngstown Sheet & Tube Co. v. Sawyer*, Supreme Court, 343 U.S. 579 (1952). (“Steel Seizure Case”).

⁹⁶¹ Steel Seizure Case. P. 635.

⁹⁶² Steel Seizure Case. P. 637.

⁹⁶³ Steel Seizure Case. P. 637.

⁹⁶⁴ Cryptome. (2 November 2013), *NSA SSO1 Slide from Guardian 13-1101*. <https://cryptome.org/2013/11/nsa-ss01-guardian-13-1101.pdf>.

In response to *Schrems II*, the NTIA whitepaper⁹⁶⁵, contains several arguments that US data importers could use during the risk analysis required by the CJEU and the EDPB. It mainly arguments that the legal situation in the US complies with the requirements of the GDPR. According to the NTIA, the EO 12333 does not authorize the US intelligence authorities to “request” access to personal data from companies. Only unilateral access, meaning “gaining access” by such authorities, is covered by EO 12333. This cannot be followed. It is true that *Schrems II* was particularly about the possibility of those authorities to request and not to provide data access. It would be a fallacy to conclude that unilateral provision of data would be irrelevant in terms of data protection law, as provision is an even more weighty interference – because it is sometimes even unnoticed – and the result is the same processing of personal data.

1.1.3. Children’s Online Privacy Protection Act

The Children’s Online Privacy Protection Act (COPPA) was introduced in 2000, with amendments taking effect in July 2013.⁹⁶⁶ It applies to the operator of any website or online service “directed to children” that collects personal data from children, or any website or online service that has actual knowledge that it is collecting personal data from children.⁹⁶⁷

The term “operator” encompasses all persons who operate a commercial website or a commercial online service and hereby collect or hold personal data or for whom such data are collected or held. Personal data are processed also if this is conducted by a representative or service provider of the operator. This also includes the case that the operator only benefits from it or that it allows another person to directly collect personal data through the website or the online service. Furthermore, COPPA applies to people who sell products across corresponding websites or online services. Another integral part of determining the area of application is the definition of “collecting” data. This means any type of request to provide personal data, but also the possibility of making personal data public, and any “passive tracking”. Although COPPA is a US-specific law, it has extraterritorial application to companies outside the US that collect personal data from children in the US.

The range of duties of the operators concerned is summarized in § 312.3 (a) to (e) with references to the following paragraphs that specify in each case. The centerpiece is the operator’s duty to obtain verifiable parental consent to the collection and use of personal data (§ 312.5). In addition, the rule also includes the requirement not to store personal data collected from children longer than necessary and then to delete it securely (§ 312.10), as well as a regulation on Safe Harbor Programs (§ 312.11). There is also the possibility under § 312.12 to address the FTC so that it confirms the COPPA conformity of the method to obtain parental consent. In addition, § 312.12 offers the possibility to request the FTC to expand the definition “support for internal operations”, which is significant in various situations.

⁹⁶⁵ Unites States Department of Commerce. (28 September 2020). *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*. <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>.

⁹⁶⁶ USA. *Children’s Online Privacy Protection Rule*, 15 U.S.C. 6501-6508, (7 January 2013). (“COPPA”).

⁹⁶⁷ Under the 2013 revisions, COPPA also applies to operators when they have “actual knowledge” that they are collecting personal information from users of another site or online service directed to kids under 13. That means that in certain circumstances, COPPA applies to advertising networks, plug-ins, and other third Parties. // See also US Federal Trade Commission. (April 2013). *Children’s Online Privacy Protection Rule: Not Just for Kids’ Sites*, <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-not-just-kids-sites#who>.

Although COPPA was an important step for children's rights in the digital environment, which was related to an increasing economic power of children, the importance for TFPD is rather small, apart from social media applications. In the US, fines can be up to USD 42,530 per COPPA violation. However, this should only be enforceable against creators from the US, since COPPA is a national law of the US. COPPA also accepts liability for US platforms for violations by foreign creators if their videos target children under the age of 13 in the US or can be reached by them. This is likely to be the case on the Internet.

1.1.4. Gramm-Leach-Bliley Act

The "Gramm-Leach-Bliley Act" (GLBA)⁹⁶⁸ was a response to data abuses in the financial sector.⁹⁶⁹ The GLBA does not constitute explicit regulation of TFPD. It nevertheless establishes data protection regulations for the financial sector and commits them to inform the respective company, for example to inform about changes to data protection regulations or to give the consumer the opportunity to opt-out. However, the law does not contain provisions for the assertion of own rights, deletion, or restrictions regarding data collection.

The GLBA has three mechanisms to ensure privacy. Firstly, financial institutions must have a privacy policy; this policy must also be communicated to the customer at the conclusion of the contract and each year thereafter. Furthermore, financial institutions are prohibited from disclosing personal data to unrelated third Parties. The data disclosure prohibition is the primary safeguard but is also subject to exceptions. § 502 GLBA regulates that – subject to other regulations – a financial institution must not disclose non-public personal data to non-affiliated third Parties, either directly or through a subsidiary, if the financial institution does not inform the consumer through a communication that complies with the requirements of § 503 GLBA. This restriction of data disclosure is – even if this is not explicitly regulated in the law – applicable to the transfer of data to third Parties abroad. Such a communication must – inter alia – disclose to whom the data may be disclosed, what happens to the information when the business relationship ends, the types of personal data collected, and the policies that the institution has in place in relation to the confidentiality and security of the data.

While the GLBA creates conditions for the protection of personal data, it also provides for several exceptions. According to § 502 (b), the data may not be disclosed unless the financial institution clearly indicates to the consumer that personal data may be disclosed and it gives them the opportunity to oppose this approach, which means that financial institutions may disclose the data if the consumer does not object, and even if the consumer makes use of the opt-out option, financial institutions may nevertheless exchange customer information with non-affiliated third Parties. This possibility is opened by § 502 (b) (2), according to which the regulation does not prevent a financial institution from disclosing information to third Parties, for example for marketing purposes, if the financial institution has a contract with this third party. Furthermore, the GLBA also contains several exceptions such as the permission to transfer personal data when selling a part of the company.

⁹⁶⁸ USA. *Gramm-Leach-Bliley Act*, 15 U.S.C. 6801-6809, (12 November 1999). ("GLBA").

⁹⁶⁹ EPIC. (January 2005). *The Gramm-Leach-Bliley Act*. <http://epic.org/privacy/glba/default.html>.

1.1.5. Internal Revenue Service Rule

Another source in the context of regulating TFPD is found in the Internal Revenue Service (IRS)⁹⁷⁰. The purpose of the new regulations adopted by the IRS, which came into effect on 1 January 2009, was to update existing regulations and to consider practices of the tax consultant industry, such as electronic preparation and filing of tax returns, expanded services and the use of resources beyond national borders. The rules contain on the one hand regulations for tax advisers about the onward transfer or use of personal data for the preparation of a tax declaration and consider explicitly the transfer abroad.

Its § 7216 and the provisions issued on this basis are intended to protect taxpayers from disclosing their personal data or using it in ways that taxpayers have not consented to. § 7216 (a) establishes legal consequences for violations of these rules. A rule initially deals with the transfer of tax information of a customer (natural or legal person) to other employees of the same tax consultant company within the US. This is possible if it is necessary to prepare the tax return. However, if the employee of the same tax consultancy company is outside the US, the data transfer is only possible with the taxpayer's consent. § 7216 requires that the taxpayer knowingly and intentionally gives its consent to that disclosure and that the consent form is dated and signed. Another rule does not concern the disclosure, but the first provision of personal data for the preparation of a tax return to a tax advisor located outside the US and the subsequent transfer of data within the company. In this case, no consent of the taxpayer to onward the data is necessary for the transfer. This derogation seems to provide an opportunity to mitigate part of the administrative burden associated with the required consent to transfer personal data abroad. For certain types of disclosure by lawyers and accountants, reference is made to § 7216 (2) (h). The regulations are particularly relevant for companies with international branches offering services to Americans living abroad or internationally operating customers, as well as generally to companies that outsource parts of their orders to other countries to save costs.

1.2. Post-9/11 instruments

Companies that operate on both sides of the Atlantic, be they EEA-based with US subsidiaries or US-based with subsidiaries in the EEA, can be contacted by US authorities to produce personal data of European data subjects. Typical scenarios are civil pre-trial discoveries but also those in connection with legal disputes of criminal or administrative nature. A variety of laws give US authorities the power to issue warrants, subpoenas, administrative orders and judicial orders that are aimed at the production of personal data in custody, possession or control of a company. These powers may also be interpreted in a way that US authorities can request the production of personal data that is stored abroad. Addressees of these requests are initially companies that are subject to US jurisdiction; however, those orders may also target personal data outside US soil.

The actual basis for data collection by US agencies abroad is FISA. The Patriot Act and the "Freedom Act"⁹⁷¹ refer to FISA as temporary amendment laws. The content of the

⁹⁷⁰ USA. *Internal Revenue Service Rule*, 26 U.S.C. § 7216, (1986). // Last amendment on 1 July 2019 by H.R. 3151.

⁹⁷¹ USA. *Public Law 114 - 23 - Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, H.R. 2048. ("Freedom Act"). // *Nota bene*: Parts of the Patriot Act expired on 1 June 2015 but were reintroduced by the "Freedom Act" on 2 June 2015 in partially modified form.

Patriot Act continues to apply in large part in modified form under the Freedom Act, which has replaced the Patriot Act in this respect.

The CJEU expressed in *Schrems II* that US authorities have extensive powers to access personal data. The ruling referred to FISA Section 702, EO 12333 and PPD-28. In the same breath alongside these laws, the Cloud Act is regularly mentioned in public. These determine the access of US authorities to personal data but are accompanied with or in relation to other legislative or executive instruments which is why we will take a closer look at them. The legal framework for the collection of intelligence from abroad is extensive and complex. The secrecy regarding the interpretation of legal powers by the NSA and other intelligence agencies, of decisions of the FISC, and the lack of public information about EO 12333 complicated the following assessment.

1.2.1. Patriot Act / Freedom Act

Since 1978, FISA has been the legal basis for electronic surveillance of foreign powers and foreign agents located in the US. FISA was amended by Section 215 of the Patriot Act in 2001. The Patriot Act was designed to provide US authorities with simplified access to personal data to foster national counter-terrorism activities after the 9/11 attacks. The Patriot Act was not a single but comprehensive amendment law that modified numerous existing US regulations. Section 215 of the Patriot Act amended 50 U.S.C. § 1861, Section 216 of the Patriot Act amended 18 U.S.C. § 3121 – a provision of the “Pen Register Act”⁹⁷² –, and Section 702 of the FISA Amendments Act amended 50 U.S.C. § 1881a.

The changes to FISA made by the Patriot Act expanded the scope of intervention that had previously existed under FISA. Central to this are Section 215 of the Patriot Act and Section 101 of the Freedom Act. “Section 215 orders may have been combined with requests under other provisions of the Patriot Act, such as Section 216, which governs access to online activity, such as e-mail contact information or Internet browsing histories”.⁹⁷³ This reference is just one example that highlights the complex interplay between different surveillance authorities. The so-called “sunset clauses”, meaning that they were set to expire after four years unless Congress reauthorized them, made this interplay even more confusing. Section 101 Freedom Act expired on 15 March 2020, so that currently Sections 501 and 502 FISA are only available as a legal basis to the reduced extent applicable before the Patriot Act. From 2006 through 2015, US Congress repeatedly reauthorized Sections 215 and 216 authorities with new sunset dates; however, these two also expired due to its sunset clause on 15 March 2020.

In the following, however, these surveillance authorities will be discussed for three reasons. Firstly, if the US Congress chooses to reauthorize these programs, “this lapse in 2020 may not have much of an overall impact”⁹⁷⁴. On the other hand, “the New York Times and others have noted that Section 215’s expiration clause contains an exception permitting the intelligence community to use the law for investigations that were ongoing at the time of expiration or to investigate “offenses or potential offenses” that occurred before the sunset”⁹⁷⁵. Third, “it is only one of a number of largely overlapping surveillance

⁹⁷² Title III within the ECPA, 18 U.S.C. §§ 3121-3127.

⁹⁷³ Brennan Center for Justice. (15 July 2013). *Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs*.

<https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf>. P. 2.

⁹⁷⁴ Electronic Frontier Foundation. (29 December 2020). *Section 215 Expired: Year in Review 2020*.

<https://www.eff.org/de/deepinks/2020/12/section-215-expired-year-review-2020>.

⁹⁷⁵ Electronic Frontier Foundation. (29 December 2020). *Section 215 Expired: Year in Review 2020*.

<https://www.eff.org/de/deepinks/2020/12/section-215-expired-year-review-2020>.

authorities⁹⁷⁶. US Congress also continued to renew Section 702 of FISA with sunset dates on a different schedule, with the next sunset date set for December 2023. Section 702 of FISA, however, does not stem from the Patriot Act and is therefore analyzed in more detail below⁹⁷⁷.

Before the Patriot Act, US authorities were only allowed to request “records” to be produced. The Patriot Act broadened this to the extent that “any tangible things” can be requested on the condition that the information within the addressees’ personal data “protect against international terrorism or clandestine intelligence activities”. Other novelties were that US authorities no longer needed to prove that a target of those intelligence activities is an agent of a foreign power and extended these powers to conceivable pieces of evidence to combat terrorism, which included US citizens being suspected of those actions. Moreover, the allowed duration of investigative activities was lengthened and any district judge in the US can since then issue surveillance orders valid not only in that respective judge’s jurisdiction but anywhere in the US. In addition, Section 215 of the Patriot Act included a “gag provision”, meaning that the recipient of such order must remain silent about having received such order. A CSP, e.g., was therefore not authorized to inform its customers that a US authority had requested the production of personal data.

Section 215 allowed authorities to obtain a FISC order requiring US “providers of electronic communications services” (as defined in 50 U.S.C. §1881 (4)), such as telephone companies, to produce any records or other “tangible thing” if deemed “relevant” to an international terrorism, counterespionage, or foreign intelligence investigation and granted US authorities access to personal data of “non-US persons”. For US intelligence agencies, a “workaround” this “non-US persons” rule was based on several points: One was the definition of “electronic surveillance”. 50 U.S.C. § 1801(f)(2) allows “the acquisition [...] of the contents of any wire communication to or from a person in the United States [...] if such acquisition occurs in the United States”. A foreign-to-foreign intelligence communication was therefore, according to the US IC’s legal theory, not “to or from a person in the United States”. When the NSA intercepted such communication, it was – at least that was this agency’s line of argumentation – not engaging in “electronic surveillance” under FISA. Another workaround was that this interception would allegedly fall into the Wiretap Act’s⁹⁷⁸ exception for foreign intelligence. FISA and ECPA establish exclusivity for 1) “electronic surveillance” and 2) interception of “domestic communications”. The third workaround played with the definition of this “domestic communication”. The rules seemed to be interpreted by the IC that a communication is only “domestic” when a communication lies wholly within the US. A US intelligence agency would have been allowed to follow the law enforcement procedures under the ECPA or the foreign intelligence procedures under FISA. Lastly, US authorities defined the term “collection” in a way that it concerns the analysis of information “after it was collected”, which enabled the IC to underreport how much its activities affect data subjects, not only US persons but also foreigners. Thus, even though the US Congress had established “exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted”⁹⁷⁹ on US soil, the NSA routinely intercepted foreign communications

⁹⁷⁶ Electronic Frontier Foundation. (29 December 2020). *Section 215 Expired: Year in Review 2020*. <https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020>.

⁹⁷⁷ Chapter III, Section II.1.2.4.

⁹⁷⁸ USA. *Omnibus Crime Control and Safe Streets Act of 1968*, Public Law 90-351, Title III, (19 June 1968). (“Wiretap Act”).

⁹⁷⁹ 50 U.S. Code § 1812. Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted.

as they passed through US networks (so-called “Transit Authority”) “to support their unwarranted collection of phone records of hundreds of millions of people in the US”⁹⁸⁰.

However, even the Patriot Act did not authorize to conduct warrantless eavesdropping on US citizens or residents in the US without an order from the FISC.⁹⁸¹ Another material requirement for carrying out such surveillance measures was that the gathering of intelligence information is a significant purpose of this activity. This included, for example, information in connection with foreign powers, groups or territories that concern a foreign matter of the US. Intelligence agencies usually issued so-called “Business Record Orders”⁹⁸², which were expanded by Section 215. A Business Record Order included a substantive judicial review, but the government “must only certify to a judge - with no need for evidence or proof - that such a search meets the statute’s broad criteria, and the judge does not even have the authority to reject the application. [...] FISA previously allowed searches only if the primary purpose was to gather foreign intelligence. But the Patriot Act changed the law to allow searches when a significant purpose is intelligence.”⁹⁸³ Investigators had then to get approval from a FISC judge and that judge then conducted a factual assessment. But the standard for a Business Record Order was “mere relevance” like a subpoena, and not “reasonable suspicion”, or “probable cause” which is listed in the Fourth Amendment of the US Constitution. The FISC did not have to make a public decision about the admissibility of the monitoring measures. Only the facts presented by the executive powers were used for the assessment of the court, without the involvement or even hearing of the data subject. So-called “*amici curiae*” were, although not obliged to, be included in the decision-making process. If the SP was requested to produce the personal data, this provider alone was entitled to a legal remedy for a renewed review of the order; data subjects did not have such right. The counter terrorism or counterintelligence investigation, or in general targeted to gather foreign intelligence information, was not to “concern” US persons. The precise meaning of that term “concern” was nevertheless not clear but seemed to cover surveillance where US persons are incidentally surveilled. A Business Record Order was therefore, compared to other types of orders, an easier way for US authorities to request the production of personal data. The NSA preferred Business Record Orders also because they did not include an obligation to notify the data subject. By using Business Record Orders for bulk surveillance programs, there was therefore statutorily less transparency and less opportunity to challenge these.

The legality of the bulk collection based on Section 215 was soon challenged in court. In “*ACLU vs. Clapper*” the court ruled that Section 215 of the Patriot Act did not authorize the bulk collection of metadata, which Judge Gerard E. Lynch called a “staggering” amount of information.⁹⁸⁴ In the political debate that followed, objections to the program largely revolved around the broad collection of metadata records from US individuals while tracking communications from non-US persons. The US press criticized the extension of the Patriot Act, particularly in times of the COVID-19 global health crisis.⁹⁸⁵

⁹⁸⁰ Karr, T. [Timothy]. (11 March 2020). *Congress Tries to Sneak Through Dangerous Spying Bill Under the Cover of the Coronavirus Crisis*. <https://www.freepress.net/news/press-releases/congress-tries-sneak-through-dangerous-spying-bill-under-cover-coronavirus>. // Due to the Snowden leaks it became public that, e.g., the reach of the PRISM program had been justified based on this provision.

⁹⁸¹ 50 U.S.C. §1803

⁹⁸² Often also called “BR orders”, “Section 215 orders”, or “Section 501 orders” (since they concern Section 501 of FISA as amended); or, since much of the early debate about Section 215 was about library records, it is also sometimes called the “library provision” of FISA.

⁹⁸³ ACLU. (23 October 2001). *Surveillance Under the USA/Patriot Act*. <https://www.aclu.org/other/surveillance-under-usapatriot-act>.

⁹⁸⁴ USA. *American Civil Liberties Union v. James Clapper*, Court of Appeals for the Second Circuit, Case 14-42, (7 May 2015).

⁹⁸⁵ E.g., Karr, T. [Timothy]. (11 March 2020). *Congress Tries to Sneak Through Dangerous Spying Bill Under the Cover of the Coronavirus Crisis*. <https://www.freepress.net/news/press-releases/congress-tries-sneak-through-dangerous-spying-bill-under-cover-coronavirus>.

Several Parliament members, led by Dutch MP Sophie in 't Veld, also opposed it.⁹⁸⁶ Amnesty International also expressed concern that counter-terrorism measures after the 9/11 attacks endangered human rights not only in the US. The delegates at the annual assembly of the German section of Amnesty International were particularly concerned about the tendency in democratic States to weaken international human rights agreements under the guise of national security; the bottom line was that the successes of the past decades could become meaningless if it is not possible to reverse this development.⁹⁸⁷ A major reform of the bulk collection program according to Section 215 would, so the opinion of those delegates, have a positive effect on the personal rights of non-US persons, whose data were also included in the bulk collection.

The Freedom Act limited US authorities' powers as a reaction to increasing public criticism. Since then, such authorities could only request records regarding a specific person, account, or device and had to present that the entity is associated with a foreign power or terrorist group. This Act also required more transparency about the data they are collecting. Recipients of such orders were no longer subjected to gag orders. It allowed citizens to lobby FISC, in practice used by civil liberties advocates challenging the US government to declassify opinions from FISC judges. But it also extended Section 215's sunset clause, made records available to the government that it had previously been unable to obtain under Section 215, and permitted the collection of records up to two steps away from a target.

If a Section 215 order related to personal data, which were stored not at the respective US group company but at a company based in the EU belonging to that US group, the question arose whether US authorities can issue an order for production of personal data to the US company or even directly to the company in the EU, in other words whether this TFPD would then be lawful from a European perspective. Developments in the US and the EU required a reassessment of this. Because, on one hand, Microsoft had meanwhile successfully defended an order before the US courts to produce e-mails to US law enforcement agencies that were stored in the Irish Microsoft subsidiary's data center.⁹⁸⁸ On the other hand, since the GDPR came into force, an unlawful transfer to US authorities and courts can in future be sanctioned with a fine of up to 4% of the concerned company's total annual turnover achieved worldwide.

Due to territorial and personal sovereignty under international law, US authorities can in principle only act within their territory and towards their nationals. This might lead to the assumption that US authorities have no possibility of assessing data collected by companies based in Europe. Understanding that these companies are solely subject to the territorial and personal sovereignty of their home State, they should be protected from the applicability of US law. The US would therefore have to rely on the assistance of the foreign State for measures that have a breakthrough on foreign territory. To be able to get such personal data from outside of the country's own territory in accordance with international law, US authorities are generally dependent on corresponding MLATs. To process the latter, legal grounds between the US and EU are laid down in the MLAT of 2003⁹⁸⁹, which later has been safeguarded by the Umbrella Agreement.⁹⁹⁰

⁹⁸⁶ European Parliament. (13 July 2011). *Question for written answer E-006901/2011*. http://www.europarl.europa.eu/doceo/document/E-7-2011-006901_EN.html.

⁹⁸⁷ Amnesty International. (27 May 2022). *Annual Report 2002*.

<https://www.amnesty.org/download/Documents/POL1000012002ENGLISH.PDF>. P. 5.

⁹⁸⁸ United States Court of Appeals for the 2nd Circuit New York. *Microsoft v. United States*, No. 14-2985, (14 July 2016).

⁹⁸⁹ EU. *Agreement on mutual legal assistance between the European Union and the United States of America*, OJ L 181, 34–40, (19 July 2003).

⁹⁹⁰ European Commission. *Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences*, OJ L 336, 3–13, (10 December 2016).

1.2.2. Tracing Terrorist Financing Program

Personal data within the EU, which are related to bank accounts, are processed according to the SWIFT program. Normally, that data would stay in Europe. The TFTP Agreement creates an exception to that and discloses certain data to the US Treasury Department. This Department then “effectively serves as an offshore service provider for the EU and European governments”⁹⁹¹. The agreement also envisaged the possible introduction of an EU system modeled on the TFTP, which would have meant a TFPD in a more targeted manner. Nevertheless, a European version of TFTP was never adopted. In 2013, the EU Commissioner for Home Affairs concluded that it would be expensive and demanding on resources to put in place and maintain. It argued that it would “require the creation of a gigantic database containing data of EU citizens’ financial transfers. Such database would raise serious challenges in terms of the data storage, access and protection, not to mention the huge technical and financial efforts”⁹⁹².

According to the agreement, data subjects can have their personal data corrected or deleted by sending a request to their competent national SA, which will transmit the request to the Privacy Officer of the US Treasury Department. Europol checks whether the data to be sent to the US are necessary for the fight against terrorism and its financial sources. Europol also ensures that the individual applications are specific enough so that as little data as possible must be requested. If these conditions are not met, no data may be transferred to the US. The US Treasury Department then “runs those searches against the TFTP data and sends the results back to Europol, which distributes them to European governments. Treasury also sends some TFTP leads directly to European governments”⁹⁹³. This procedure under Art. 4 TFTP has been analyzed by the EDPS, which concluded that “overall, Europol manages well the verifications of the US DoT requests. The different actors complement each other and pay close attention to details. The EDPS has identified good practices when Europol analyzes the US requests”⁹⁹⁴.

The TFTP Agreement offers enhanced data protection guarantees with regard to transparency, access rights and the correction and deletion of incorrect data. It guarantees official remedy without distinction and ensures that every person whose data are processed under the agreement can appeal to courts in the US against an administrative measure adversely affecting them. In addition, the principle of proportionality is recognized as the guiding principle for the application of the agreement.

On 22 July 2019, the Commission presented a Report on the TFTP Agreement. Therein, the Commission resumed to be “satisfied that the Agreement and its safeguards and controls are properly implemented”⁹⁹⁵. To the same conclusion reached the PCLOB: “The Board’s review indicates that TFTP is thoughtfully designed, provides significant

⁹⁹¹ US Privacy and Civil Liberties Oversight Board. (2020). *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*. https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%202011_19_20.pdf. P. 1.

⁹⁹² European Commission. (27 November 2013). *Speech - EU-US agreements: Commission reports on TFTP and PNR*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_13_985.

⁹⁹³ US Privacy and Civil Liberties Oversight Board. (2020). *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*. https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%202011_19_20.pdf. P. 2.

⁹⁹⁴ EDPS. *Case number: 2018-0638, 28 May 2019*. https://edps.europa.eu/sites/edp/files/publication/19-05-28_edps_inspection_report_art4_tftp_en.pdf, (28 May 2019). P.1. // Recommendations of the EDPS suggest improving the exchange of information between US and EU authorities, to increase visibility of changes in the annual reports, and to destroy requests and verification forms older than 5 years.

⁹⁹⁵ European Commission. *Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, SWD(2019) 301 final, (22 July 2019). P. 19

value for counterterrorism, and appropriately protects individual privacy. The recommendations provided to the Department of the Treasury, which administers TFTP, will reinforce the program's privacy safeguards. [...] The bottom line is that this program, though funded and operated by the United States, provides a steady stream of valuable intelligence to EU member states."⁹⁹⁶ Nevertheless, the PCLOB stated also that the "EU has effectively deputized the U.S. Treasury to perform counterterrorism searches of European data."⁹⁹⁷ With this letter the US reacted to emerging criticism of TFTP from, for example, the Parliament, as the Union, according to the argumentation of the US, benefits from the results of the TFTP data analysis carried out in the US and had opted against an EU-owned program similar to TFTP.⁹⁹⁸ The EDPB replied to this view by concluding that the current procedure "might however result in a situation where the data subject is not informed of whether her or his data are stored in the TFTP database or whether any breaches to the agreement had to be remedied in response to her or his request. This broad and unverified restriction to the exercise of the right of access – expressly and specifically recognized as a fundamental right in Article 8(2) of the EU Charter of the Fundamental Rights – clearly prejudices the exercise of the other data subject's rights"⁹⁹⁹. The EDPB "considers these provisions to be insufficient. In its *Schrems II* ruling, the CJEU stressed again – in the context of personal data transfer to third countries – the importance and necessity of ensuring data subjects' rights' enforceability against authorities in the courts, in order to provide for an effective judicial remedy".¹⁰⁰⁰ The EDPB proposed "to improve the process in general and provide for some accountability".¹⁰⁰¹ Regarding the retention period of unextracted data, the EU had initially agreed to store these data for five years. However, it made this dependent on a review within three years of the entry into force of the agreement as to whether the retention period should be shortened. The EDPB repeated its concern regarding the data retention period: "It follows from the Agreement that non-extracted data may be retained for five years. Such retention of non-extracted financial information continues to be of great concern to the EDPB, as it is also very problematic in view of the jurisprudence of the Court of Justice of the European Union".¹⁰⁰² The EDPB therefore reiterated "its call to review not only the PNR agreements, which face similar problems, but also the TFTP agreement with the United States".¹⁰⁰³

⁹⁹⁶ US Privacy and Civil Liberties Oversight Board. (2020). *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*. https://documents.pcllob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf. P. 3.

⁹⁹⁷ US Privacy and Civil Liberties Oversight Board. (2020). *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*. https://documents.pcllob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf. P. 4.

⁹⁹⁸ European Parliament. (23 October 2013). *MEPs call for suspension of EU-US bank data deal in response to NSA snooping*. <https://www.europarl.europa.eu/news/en/press-room/20131021IPR22725/meps-call-for-suspension-of-eu-us-bank-data-deal-in-response-to-nsa-snooping>. // US Privacy and Civil Liberties Oversight Board. (2020). *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*. https://documents.pcllob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf. P. 14.

⁹⁹⁹ EDPB. *Letter with Ref. OUT2020-0131*, https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0131_reply_letter_on_tftpagreement.pdf, (3 December 2020). P. 1.

¹⁰⁰⁰ EDPB. *Letter with Ref. OUT2020-0131*, https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0131_reply_letter_on_tftpagreement.pdf, (3 December 2020). P. 2.

¹⁰⁰¹ EDPB. *Letter with Ref. OUT2020-0131*, https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0131_reply_letter_on_tftpagreement.pdf, (3 December 2020). P. 2.

¹⁰⁰² EDPB. *Letter with Ref. OUT2020-0131*, https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0131_reply_letter_on_tftpagreement.pdf, (3 December 2020). P. 2.

¹⁰⁰³ EDPB. *Letter with Ref. OUT2020-0131*, https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0131_reply_letter_on_tftpagreement.pdf, (3 December 2020). P. 3.

In its last review of the TFTP Agreement, the Commission is “overall satisfied that the Agreement and its safeguards and controls are properly implemented”¹⁰⁰⁴. Reactions of the EDPS and others to this Report could not be included in this thesis.

1.2.3. National Security Letters

A NSL is a law enforcement tool under US law, authorized by the SCA. A NSL is used by the FBI – in limited circumstances also by other federal agencies – to demand that companies produce data that is “relevant” to authorized national security investigations. Title V of the Patriot Act has significantly expanded the scope of the NSL. In 2006, US Congress included a provision that a NSL recipient can petition a federal district court to modify or set aside both the NSL and the gag order that might accompany such demand; this possibility must also be communicated to the recipient. The Freedom Act in 2015 amended the NSL tool again and included a provision on termination. A NSL can be used against US citizens and foreigners on US soil. A possible gag order can also be applied to a NSL, 18 U.S.C. § 2709(c).

There are only two requirements for issuing a NSL. Firstly, there must be an approval by a senior FBI official¹⁰⁰⁵, 18 U.S.C. § 2709. This deviates from the normal process that US federal investigators need a subpoena issued by a grand jury because they do not have administrative subpoena power. In the case of a NSL, no court is involved in the process, so a NSL can be seen as administrative subpoena. NSLs became therefore a more important measure to the executive branch compared to Business Record Orders.¹⁰⁰⁶ Secondly, according to 18 U.S.C. § 2709, it is sufficient that the requested data are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.” The scope of the data categories requested via a NSL is limited to customer’s name, address, length of service, communications records, and banking and other financial and credit information, and content data cannot be requested. A NSL is restricted to certain recipients, such as credit reporting agencies, telecommunications providers, financial institutions and travel agencies.

ISPs began to resist a broad interpretation of the NSLs and stopped giving out electronic messaging metadata in response to NSLs. The FBI therefore began to rely more on Business Record Orders. Nevertheless, the total number of NSLs in the US has risen constantly.¹⁰⁰⁷

A legal proceeding against a NSL is not easy in practice because the FBI generally argues that, for reasons of national security, the NSL must remain secret. Nevertheless, the case of CREDO Mobile, a California-based telecommunications company, which filed a legal complaint against a NSL, became public.¹⁰⁰⁸ The FBI filed a counterclaim and

¹⁰⁰⁴ European Commission. *Report from the Commission to the European Parliament and the Council, On the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, COM(2022) 585 final, (11 November 2022). P. 2.

¹⁰⁰⁵ FBI Director, FBI Assistant Director, or FBI Special Agents in charge.

¹⁰⁰⁶ EPIC. (2022). *FISA Orders: 1979-2020. FISA Court Orders and National Security Letters Issued*. <https://epic.org/privacy/surveillance/fisa/graphs>.

¹⁰⁰⁷ Electronic Frontier Foundation. (1 December 2016). *Fighting NSL Gag Orders, With Help From Our Friends at CREDO and Internet Archive*. <https://www.eff.org/de/deepinks/2016/12/fighting-nsl-gag-orders-help-our-friends-credo-and-internet-archive>.

¹⁰⁰⁸ Electronic Frontier Foundation. (30 November 2016). *CREDO Confirms It’s at Center of Long-Running Legal Fight Over NSLs*. <https://www.eff.org/press/releases/credo-confirms-its-center-long-running-nsl-fight>.

argued that the filing of the complaint as such would violate US national security interests. In July 2017, the Ninth Circuit issued an opinion upholding the NSL tool. The court ruled that the NSL tool survived strict scrutiny and that it included all procedural protections required of prior restraints, holding that a NSL is constitutional.¹⁰⁰⁹

1.2.4. FISA Amendments Act

Section 702 was first enacted as part of the FISA Amendments Act of 2008 and reauthorized during the Obama administration in 2012.¹⁰¹⁰ FISA was extended in 2018, limited to six years.¹⁰¹¹ The purpose of Section 702 is “to close the gap between the collection of non-U.S. person communications outside the United States (which is governed by Executive Order 12333) and the collection of U.S. person communications inside the United States (which is governed by “traditional” FISA. [...] The question is not where the provider is located; it’s where the data is located.”¹⁰¹²

US intelligence services intercepting “foreign-to-foreign” (that originates and terminates in foreign countries) personal data as it transits the US, is in principle not covered by either FISA or the ECPA, but only by EO 12333. However, there are “areas where the NSA collects data outside the United States, but under FISA”¹⁰¹³. If the data are stored by US companies (including their EU subsidiaries) outside the US, these data may indeed fall under Section 702 whenever a US authority intercepts a wireless communication outside the US and all the Parties to that communication are inside the US, being the final target of surveillance. Thus, the division between FISA Section 702 and EO 12333 also depends on the communications medium, the location of the Parties to the communication, and the US personhood of the target. Jonathan Mayer therefore perfectly noted that “that’s the conventional wisdom. American soil: FISA. Foreign soil: EO 12333. Unfortunately, the legal landscape is more complicated”¹⁰¹⁴, which also his graphic showcases.

¹⁰⁰⁹ “The nondisclosure requirement does not run afoul of the First Amendment.” US Court of Appeals Ninth Circuit. *Seal v. Jefferson B. Sessions III*, Cases No. 16-16067, 16-16081, and 16-16082, (17 July 2017). Para. 43.

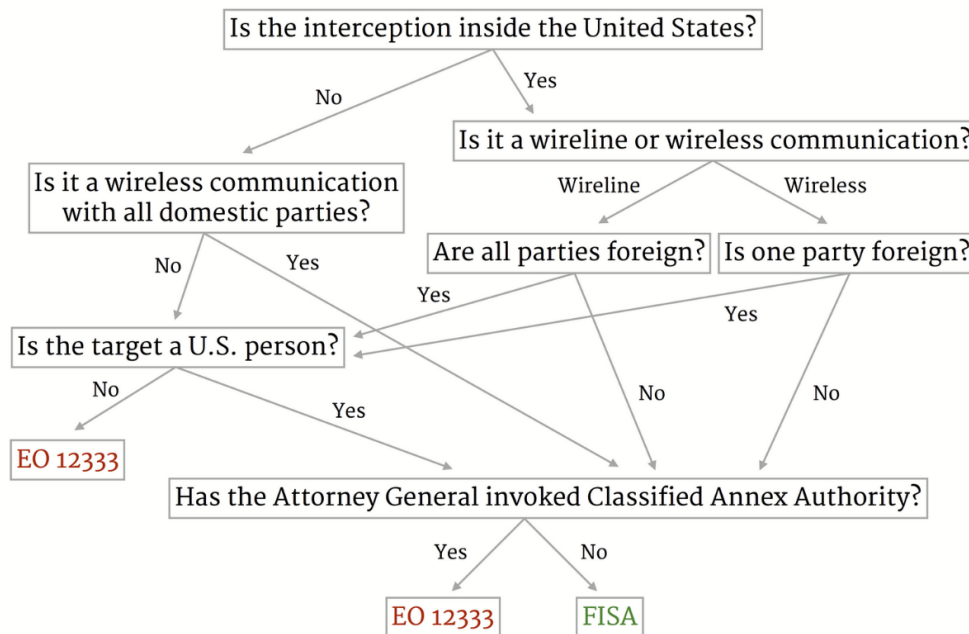
¹⁰¹⁰ Unites States of America. *FISA Amendments Act of 2008*, H.R. 6304, (10 July 2008). // Unites States of America. *FISA Amendments Act Reauthorization Act of 2012*, H.R. 5949, (30 December 2012).

¹⁰¹¹ USA. *S. 139 - FISA Amendments Reauthorization Act of 2017*, (19 January 2018).

¹⁰¹² Conference of German Independent Data Protection Supervisors of the Federal Government and the States. (15 November 2021). *Expert Opinion on the Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladeck, University of Texas School of Law*. https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladeck_Rechtsgutachten_DSK_en.pdf. P. 8–9.

¹⁰¹³ Mayer, J. [Jonathan]. (3 December 2014). *Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier*. <http://webpolicy.org/2014/12/03/eo-12333-on-american-soil>.

¹⁰¹⁴ Mayer, J. [Jonathan]. (3 December 2014). *Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier*. <http://webpolicy.org/2014/12/03/eo-12333-on-american-soil>.



Source: Mayer, Jonathan, "Intercepting Communications Content: FISA or EO 12333?"¹⁰¹⁵

Section 702 aims at non-US persons reasonably believed to be located outside the US by issuing “directives” to collect “all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition”. Many of these terms are ambiguous, at least to some degree. The expert opinion of Vladeck¹⁰¹⁶ showed that Section 702 covers all electronic communications, both stored and prospective data, including metadata as well as content, and both data in transit (“upstream”) and data at rest (“downstream”).¹⁰¹⁷ In addition, the term “electronic communication service provider” is to be understood very broadly, and not only “classic IT and telecommunications companies” can be included; included are also, among others, providers of “remote computing services” and not only conventional telecommunications providers. Also, access by US authorities is not limited to data related to this service, but even a minor activity opens the scope of FISA 702 to all data in the targeted company, even if this SP has nothing to do with the main entrepreneurial activity.

A Section 702 procedure starts with the Attorney General and the DNI submitting a filing to the FISC. That filing includes a certification that among other things a “significant purpose” of the surveillance will be to gather foreign intelligence. The US authorities requesting the surveillance do not need “probable cause” or “reasonable articulable suspicion” or even “relevance”, nor does there have to be a foreign power or an agent of a foreign power targeted. This illustrates the exceedingly wide variety of purposes. The filing has also to include certain “targeting procedures” established to ensure that the government is targeting people “reasonably believed” to be outside the US. In addition,

¹⁰¹⁵ Mayer, J. [Jonathan]. (3 December 2014). *Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier*. <http://webpolicy.org/2014/12/03/eo-12333-on-american-soil>.

¹⁰¹⁶ Conference of German Independent Data Protection Supervisors of the Federal Government and the States. (15 November 2021). *Expert Opinion on the Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladeck, University of Texas School of Law*. https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

¹⁰¹⁷ Conference of German Independent Data Protection Supervisors of the Federal Government and the States. (15 November 2021). *Expert Opinion on the Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladeck, University of Texas School of Law*. https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf. P. 2–3.

the authority must adopt “minimization procedures” to guard against inadvertent collection, retention, and dissemination of personal data about US persons, but the executive branch does not have to prove how it will avoid this effect. A FISC judge then assesses whether the certification and procedures are statutorily sufficient and can request changes to the measure. Once the judge is satisfied, he/she issues a so-called “Section 702 Order”, valid for one year. Once the requesting authority has obtained this Section 702 Order, it can issue “Section 702 Directives” within one year. Those function alike warrants or wiretap orders without a court being involved. There are two types of Section 702 Directives that the Department of Justice (DOJ) has sought to issue. The first type is a “Targeted Directive”, which is targeted to a particular technology service associated with certain user accounts. The PRISM program was an instance of that Targeted Directive. The second type is a “Bulk Surveillance Directive”. The program associated with Section 702 Directives of this second type is usually named “Upstream Collection”. An order issued under Section 702 may require a provider to disclose personal data to, or provide access to, a US intelligence agency. But it is the Section 702 Directive that finally compels the disclosure. Section 702 by itself does not require such providers to proactively disclose data or provide general access to these data to US intelligence agencies. Nevertheless, Section 702 is mandatory in the sense that an entity targeted by such Section 702 Directive then must either (1) comply with the directive or (2) challenge the directive in FISC.

US courts and authorities interpret the rules of FISA extensively in such a way that parent companies as well as their subsidiaries in the US can be required to produce personal data from their parent or subsidiary companies abroad (e.g., in Europe). The question when a US company “owns”, “holds”, or ultimately “controls” certain data is differently approached. It is not uncommon for US courts to consider it irrelevant whether an international agreement exists with a foreign country on the production of such data¹⁰¹⁸, and whether the data are held by the US company itself, a subsidiary or parent company or, as often the case with cloud services, by third Parties, e.g., external SPs. US courts regularly assume ownership or control of data by US companies if the US company either has the “legal right to obtain the data” or has the “technical ability to access the data”.¹⁰¹⁹ As far as the production of data from third Parties – meaning companies not affiliated with company law – is concerned, US courts assume at least “control” over the third party, if the third party has any kind of contractual obligation due to the group structure. Occasionally, US courts even consider delivering production orders with a corresponding effect directly to subcontractors or SPs.¹⁰²⁰ Some courts only check whether a US company actually has access to the data; then it is not decisive whether that US company has “legal ownership” of the data or physical possession of it but sufficient that this US company has access (“access to the documents”) and the ability to achieve them (“ability to obtain them”).¹⁰²¹ However, a contractual commitment and regular joint business activity or connection (“regular course of business”) to the corresponding third party is regularly required.

These powers of US authorities are used on a regular basis, as emphasized by those which increasingly offer cloud services.¹⁰²² The consequence for CSPs would be that

¹⁰¹⁸ USA. Court of Appeals for the 2nd Circuit New York, *Judgment of 14 July 2016*, Case No. 14–298, (14 July 2016).

¹⁰¹⁹ USA. *Banken Trust Co.*, US Court of Appeals for the Sixth Circuit, 61 F.3d 465 [469], (3 August 1995). // USA. *Linde v. Arab Bank, PLC*, US District Court, E.D. New York, 262 F.R.D., 136 [139], (22 May 2009).

¹⁰²⁰ USA. *Kelley v. Euromarkiet Designs, Inc.*, US District Court, E.D. California, No. Civ S-07-2302, (7 January 2008).

¹⁰²¹ USA. *Hunter Douglas, Inc. v. Comfortex Corp.*, No. Civ. 98 Civ. 479, (3 March 1999).

¹⁰²² Gordon Frazer, the managing director of Microsoft UK, said that he could not guarantee that the data stored on Microsoft servers, wherever they were, would not be in the hands of the US Government. See Whittaker, Z. [Zack]. (28 June 2011). *Microsoft admits Patriot Act can access EU-based cloud data*. <https://www.zdnet.com/article/microsoft-admits-patriot-act-can-access-eu-based-cloud-data>. // Google also pointed this out on 12 January 2022 in its Privacy Policy: “We’ll process your data when we have a legal obligation to do so, for example, if we’re responding to legal process or an enforceable governmental request.”, <https://policies.google.com/privacy?gl=en&hl=en#infodelete>.

personal data in the cloud are subject to US law. Even if they conclude an commissioned data processing agreement with a European contractor, there would be a risk that the third party (the contractor) is subject to US authorities' powers. If such third party is covered by the scope of Section 702, it may issue the requested documents based on its fear of possible sanctions, even if this would mean a breach of a contract with its client. In a worst-case scenario, this could result in data processing contracts falling within the scope of Section 702 – regardless of whether the SPs are based in the US or through a group-structure link with US companies.

FISA has therefore been criticized for years in Europe, arguing that Section 702 does not afford foreign individuals enough protection and that it involves “bulk collection” (untargeted collection of all records). The EU Commission also explicitly stated in its first annual report on the Privacy Shield:

The upcoming debate on the re-authorization of Section 702 of the Foreign Intelligence Surveillance Act (FISA) provides the U.S. Administration and Congress with a unique opportunity for strengthening the privacy protections contained in FISA. In this context, the Commission hoped that the Congress will consider favorably enshrining the protections offered by Presidential Policy Directive (PPD)-28 with respect to non-US persons in FISA, with a view to ensuring the stability and continuity of these protections. Any further reforms, both in terms of substantive limitations and in terms of procedural safeguards, should be implemented in the spirit of PPD-28 and thus provide protection irrespective of nationality or country of residence.¹⁰²³

When a US authority conducts extensive surveillance of foreign individuals and businesses, it necessarily conducts extensive surveillance on US persons as a formal legal matter. Through Section 702, US-persons could therefore also have their communications intercepted by surveillance programs operated by US authorities, which could violate the Fourth Amendment's protection against unreasonable searches and seizures.¹⁰²⁴ Proponents of FISA nevertheless defended it as an important tool to prevent terrorist attacks and that European intelligence agencies would also benefit from FISA for their anti-terrorist actions carried out together with US authorities. The NTIA found in a whitepaper¹⁰²⁵ that the CJEU had not considered some of the (positive) changes made in Section 702 after July 2016; therein, it further argued that

- permanent judges panel of the FISC can enforce compliance with the targeted requirements of Section 702 FISA and does so in practice by imposing data protection measures;
- FISC has made it clear that its review of the Section 702 procedures is not limited to written procedures, but also includes how the government implements those procedures;
- there is evidence that the FISC plays an active role in monitoring whether individuals are legally targeted for information from the International Intelligence Services;
- the role of the FISC in approving and monitoring decisions targeting Section 702 is seen as advantageous compared to comparable intelligence programs in the EU;

¹⁰²³ European Commission. *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield*, COM(2017) 611 final. P. 6

¹⁰²⁴ “But the law gives the intelligence community space to target foreign intelligence in ways that inherently and intentionally sweep in Americans' communications. [...] “The bill that was most recently passed, S. 139, endorses nearly all warrantless searches of databases containing Americans' communications collected under Section 702. It allows for the restarting of “about” collection, an invasive type of surveillance that the NSA ended in 2017 after being criticized by the Foreign Intelligence Surveillance Court for privacy violations.” See EFF. (2023). *Decoding 702: What is Section 702?*. <https://www.eff.org/702-spying>.

¹⁰²⁵ United States Department of Commerce. (28 September 2020). *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*. <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>.

- before the US government may access communications data of an individual (including an EU citizen or EU resident) who complies with certain destination restrictions, unless otherwise compelling circumstances, it must file a request to the FISC for written approval (Section 702 order). The approval is limited, timewise to a period of up to a year, and purpose-wise to a specific type of foreign intelligence service, e.g., terrorism or the acquisition of weapons of mass destruction;
- a review of applicable US law shows that several US laws give individuals of any nationality the right to remedy violations of FISA – including violations of Section 702 – through civil actions before US courts;
- PPD-28 measures are subject to the supervision of various US authorities;
- most companies do not process data that would be of interest for intelligence purposes. Therefore, in effect, those companies do not have to fear such access as outlined in the CJEU ruling;
- the US government regularly shares intelligence with EU Member States that serves to combat terrorism, illicit arms trafficking, and hostile cyberattacks. The powers are thus in the interest of EU members;
- US security agencies' access rights are not significantly different from the access rights that other States, including EU Member States, obtain for their agencies. Moreover, the NTIA argued the access rights of security authorities elsewhere are not regulated at all, or at least not as thoroughly as in the USA.

The NTIA's opinion regarding Section 702 cannot be followed for the following reasons. On the one hand, the powers of government agencies are too vague and disproportionate in relation to the protected rights concerned. As the ECtHR made clear, the facts of authorization must be structured comprehensively, predictably and restrictively in secret surveillance procedures.¹⁰²⁶ The regulations in FISA do not objectively foresee whether and to what extent foreigners could be affected by the surveillance measures. On the other hand, there are no restrictions regarding the information concerned. Once a possible connection to intelligence activities has been established, any information that reaches one or more communication channels can be intercepted. Moreover, due to the secret proceedings of FISC, judicial control is only an option if the individual affected gains sufficient knowledge of the monitoring in a later procedure. Legal protection measures must nevertheless be available to the individual in situations in which, due to the confidentiality of the surveillance, it has no or no sufficient knowledge of his own concern. It should also be noted that this protection lapses if the plaintiff can only submit a suspicion, but no substantiated facts, that it is the victim of a surveillance. This applies particularly if the plaintiff has no reliable documents available for a judicial process, which ultimately can lead to an interference with the right to a fair trial. A notification of the surveillance measure to the data subject is only provided if the intercepted data are used against this subject in a later procedure, not if surveillance remains unsuccessful. This lack of information on the part of the plaintiff can be exacerbated by the so-called "state secrets privilege" in US law. The most important case on the FISA issue related to this privilege, *FBI v. Fazaga*¹⁰²⁷, was recently decided by the US Supreme Court. One of the issues this case raised was whether FISA overrides the state secrets privilege in cases where plaintiffs allege that their communications were unlawfully intercepted in violation of FISA. FISA provides a procedure for judicial review of whether classified information can and should be admitted into evidence. The Supreme Court held that Sec. 1806(f) FISA does not override the state secrets privilege. The court unanimously suggested that the state secrets privilege is rooted in the US Constitution, not the common law, and is therefore protected from regulation or abrogation by US Congress. Since there is insufficient and

¹⁰²⁶ ECtHR, *Roman Zakharov v. Russia*, Judgment of 4 December 2015, Application no. 47143/06. Para. 302

¹⁰²⁷ US Supreme Court. *Federal Bureau of Investigation et al v. Fazaga et al*, No. 20-828, (4 March 2022).

independent judicial control by the FISC, FISA interferes disproportionately with the fundamental right to effective legal protection.

From a European perspective, it should therefore be noted that the problem of Section 702 in cloud computing scenarios would not simply be solved by storing the data in a European cloud. Voigt¹⁰²⁸ also assumes a potentially worldwide reach of US authorities. In principle, even a loose connection between an addressee and the US could be sufficient to be subject to US regulations. Not only are US companies covered, but also their subsidiaries abroad. Conversely, even US subsidiaries or sister companies of foreign companies could be required to exercise their rights of influence within the group structure to achieve data disclosure. It could even be sufficient for a European company to maintain an office in the US as a connecting factor. When considering whether to cooperate with the US authorities or to act against such an order, long-term commercial interests are therefore likely to play a role, particularly with contract data processors. Critics of Section 702 in Europe must nonetheless recognize that there have also been legal efforts in the EU in accessing data on counterterrorism to the benefit of European security agencies. The EU “Data Retention Directive”¹⁰²⁹ provided means to fight crime in certain cases that had no counterpart in the US, although this Directive has been annulled by the CJEU in 2014.¹⁰³⁰

1.2.5. Presidential Policy Directive 28 and Executive Order 14086

A change in US government policy regarding the collection of foreign intelligence and data protection standards for non-US individuals occurred in 2014 with PPD-28. PPD-28 wants to restore legitimacy through transparency, oversight and higher standards to protect personal data and to limit the use of signal intelligence (US SIGINT) tools to specific purposes. It addresses intelligence agencies to improve the inequality of treatment between Americans and foreigners.¹⁰³¹

The main innovations of PPD-28 related to the protection of personal data of foreigners are as follows:

- PPD-28 determines exclusive purposes for which a bulk collection of SIGINT can be permitted.
- PPD-28 prohibits the collection of foreign intelligence information for the purpose of suppressing political opposition or to discriminate people based on ethnicity, race, gender, sexual orientation or religion. All persons are to be treated with dignity and respect, regardless of their nationality or place of residence, and all persons have a legitimate interest in their privacy when processing their personal data. SIGINT activities must therefore include adequate safeguards for the personal data of all natural persons, regardless of the nationality of the individual to whom the information relates or where they live.
- PPD-28 prohibits the collection and dissemination of intelligence information for the commercial benefit of US business interests.

¹⁰²⁸ Voigt, P. [Paul]. Weltweiter Datenzugriff durch US-Behörden – Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten. *MMR* 2014(3), 158–161.

¹⁰²⁹ European Commission, Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 13 April 2006, OJ L 105, pp. 54–63

¹⁰³⁰ CJEU. Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

¹⁰³¹ “Regardless of the nationality of the individual to whom the information pertains or where that individual resides”, Office of the Director of National Intelligence, “Status of Implementation of PPD-28: Response to the PCLOB’s Report, October 2018”, p. 1, <https://irp.fas.org/offdocs/pclob-ppd28-response.pdf>.

- PPD-28 instructs the IC to apply their data protection standards and safeguards to the greatest possible extent that is compatible with national security for all persons, regardless of their nationality. This includes a minimization process that limits the retention of personal data to 5 years and the distribution of personal data to the standard that also applies to comparable personal data from US persons. Personal data must be kept in secure conditions to prevent unauthorized access, and personal data are only used in the intelligence reports if these data have a specific international intelligence value. This Section also prescribes a renewed emphasis on supervision and mandates a series of reports on the implementation of these guidelines by the IC.
- PPD-28 also instructs the Secretary of State to appoint a senior official to act as an interface with any foreign government who wishes to raise concerns about US SIGINT.

Although PPD-28 is a promising document which sets safeguard principles for the protection of foreign persons' personal data, with which norms for the legal legitimacy are to be established, criticism must also be outlined in the following. It is unclear what practical effects PPD-28 has, since it addresses instructions to the authorities, which are ultimately responsible for implementing those principles. It is also significant that parts of PPD-28 are only specified in a classified annex, which makes a reliable assessment difficult. In *Schrems II*, the CJEU identified various deficiencies in PPD-28, which contradict Art. 45(2)(a) GDPR. The requirements of PPD-28 do not give data subjects rights that could be enforced in court against US authorities.¹⁰³² This deficiency is not remedied by the ombudsman mechanism provided, because it does not meet the criteria of Art. 47 of the Charter, as the ombudsperson is not sufficiently independent from the US executive. In addition, PPD-28 allows the collection of a large amount of US SIGINT under conditions in which the IC cannot use an identifier associated with a specific target person for a targeted survey. The Commission also expressed concern and suggested in its first report on the Privacy Shield that the protections provided for in PPD-28 for people outside the US should be anchored in the FISA and that the report of the PCLOB on the application of the PPD-28 should be released to the public.¹⁰³³

PPD-28 remained in full effect until the "Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities" (EO 14086)¹⁰³⁴ of POTUS Biden. EO 14086 stated that "The head of each element of the Intelligence Community: (A) shall continue to use the policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014 (Signals Intelligence Activities) (PPD-28), until they are updated pursuant to subsection (c)(iv)(B) of this section." This section states that a head of each element of the Intelligence Community "shall, within 1 year of the date of this order, in consultation with the Attorney General, the CLPO, and the Privacy and Civil Liberties Oversight Board (PCLOB), update those policies and procedures as necessary to implement the privacy and civil liberties safeguards in this order"¹⁰³⁵.

¹⁰³² "But PPD-28's limits do not turn on whether the collection is or is not consistent with EU or EU member state law (they turn, instead, on the underlying purposes of the collection). And in any event, PPD-28 does not create any enforceable rights that a U.S. electronic communication service provide or a non-U.S. subsidiary of such a provider could enforce in court." // Conference of German Independent Data Protection Supervisors of the Federal Government and the States. (15 November 2021). *Expert Opinion on the Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladek, University of Texas School of Law*. https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf. P. 8.

¹⁰³³ European Commission. (18 October 2017). *EU-U.S. Privacy Shield: First review shows it works but implementation can be improved*. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3966.

¹⁰³⁴ USA, The White House. *Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*, <https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence>, (7 October 2022). ("EO 14086").

¹⁰³⁵ USA, The White House. *Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>, (7 October 2022). Sec. 2. (c)(iv)(B).

EO 14086, which had emerged in the course of negotiations between the EU and the US on a new “Transatlantic Data Privacy Framework”¹⁰³⁶ since the beginning of 2022,¹⁰³⁷ “limits access of US intelligence agencies to what is ‘necessary’ and ‘proportionate’ to protect national security; increases oversight for the activities of US intelligence agencies to ensure compliance; and establishes independent and impartial redress mechanisms, including the new Data Protective Review Court tasked with investigating and resolving complaints by Europeans who have had their personal data accessed by US national securities.”¹⁰³⁸ However, NOYB criticized that EO 14086 “seems to fail on both requirements, as it does not change the situation from the previously applicable PPD-28. There is continuous bulk surveillance and a court that is not an actual court. Therefore, any EU adequacy decision that is based on Executive Order 14086 will likely not satisfy the CJEU.”¹⁰³⁹

1.2.6. Judicial Redress Act

The *Schrems II* case underlined that a future durable arrangement for data transfers between the EU and the US would require the improvement of two points, which the CJEU identified in which US surveillance law lacks essential equivalence to EU safeguards. That the US legal framework lacks, firstly, an “effective and enforceable” right of individual redress, and secondly “proportionality” in the scale of US intelligence activities. The former is a matter of substance, the latter a matter of governance.

The JR Act aims at granting foreign nationals of certain nationalities the same rights as US citizens vis-à-vis US authorities. The JR Act extended the Privacy Act remedies to citizens of so-called “covered countries”¹⁰⁴⁰. Citizens of EU countries who are facing an alleged infringement of their rights, can now appeal before those courts in the US which are tied to the JR Act. Nevertheless, because the JR Act is tied to the Privacy Act, foreigners can only sue if the privacy policies of the Privacy Act are violated. On the other hand, if federal agencies violate privacy regulations that are not governed by the Privacy Act, foreigners have no right to a remedy.

The JR Act is related to the Umbrella Agreement. Art. 19(1) of the Umbrella Agreement provides EU citizens with rights to judicial redress. Prior to the JR Act, the Commission expected from the US lawmakers

that all designations under that [JR] Act, both of the EU as a “covered country” and of all U.S. agencies that process data falling within the scope of the Agreement as “designated federal agency or component”, will be made and that all data transfers falling within the scope of the Umbrella Agreement will be covered. The Commission confirms that this includes transfers carried out on the basis of the EU-US Agreement on Passenger Name Records (PNR) and the EU-US Agreement on the processing and transfer of Financial Messaging Data from the EU to the U.S. for purposes of the Terrorist Finance Tracking Program (TFTP) (see Article 3(1) in conjunction with the fourth paragraph of the preamble to the Agreement) and that the respective datasets cannot be exempted from the benefit of the judicial redress rights granted by the JR

¹⁰³⁶ Since 3 July 2023 in place as the “EU-US Data Privacy Framework”, see EPILOG

¹⁰³⁷ See Chapter IX, Section II.1.

¹⁰³⁸ Dentons Kensington Swan. (19 July 2023). *Latest instalment in EU-US Data Protection Framework—will it stand?*. <https://www.dentons.co.nz/en/insights/articles/2023/july/17/latest-instalment-in-eu-us-data-protection-framework>.

¹⁰³⁹ NOYB. (13 December 2022). *Statement on US Adequacy Decision by the European Commission*. <https://noyb.eu/en/statement-eu-commission-adequacy-decision-us>.

¹⁰⁴⁰ 28 covered countries as of 13 January 2022. See US Department of Justice. (28 December 2022). *Judicial Redress Act of 2015 & U.S.-EU Data Protection and Privacy Agreement*. <https://www.justice.gov/opcl/judicial-redress-act-2015>.

Act. The Commission considered that only this would ensure the full implementation of Art. 19 (1) of the Agreement as required by Article 5(2) and (3) of the Agreement.¹⁰⁴¹

However, EPIC criticized in a letter to the House Judiciary Committee that the JR Act does not provide the same basis for legal actions for non-US persons as it does for US persons, for the following reasons:

First, it limits the scope of the Privacy Act's catchall provision, § 552a(g)(1)(D), to only intentional or willful violations of § 552a(b), which prohibits disclosure of personal information without consent unless the disclosure is subject to the enumerated exceptions. Under the bill, non-U.S. persons will not be able to sue agencies for failure to comply with any other provision of the Privacy Act, nor will they be able to sue for an agency's violation of its own regulations. Second, the bill substantially limits a non-U.S. person's ability to sue an agency for failure to amend a record or refusal to provide access to a record. According to H.R. 1428, non-U.S. persons will only be able to sue "designated agencies" for refusal to provide access to or for failure to amend a record. Federal agencies that are not "designated agencies", but which maintain records on non-U.S. persons fall outside the scope of the Act's provisions. Finally, non-U.S. persons have no ground to challenge an agency for an adverse decision – such as a denial of a visa or refugee resettlement application – when the adverse decision resulted from the agency's failure to maintain their records with the requisite accuracy, relevance, timeliness, and completeness necessary for fair determinations.¹⁰⁴²

In addition, a non-US person will only be able to sue a designated agency for "improper disclosure" of its personal data. Furthermore, an appeal to the JR Act can only be considered if the data are transferred directly from a public or private body from the EEA to a US authority. Only records received by the US from the "covered country" will receive Privacy Act protections; other non-US citizens personal data received from other countries or otherwise obtained by the relevant agency will remain unprotected. This extends discretion to members of the executive branch to select, which non-US persons will enjoy protections under the Privacy Act. The CIA and the FBI, e.g., were not put on the list of such "Designated Federal Agencies and Components".¹⁰⁴³ If the EU or a specific EU country prohibits the transfer of personal data to the US for commercial purposes, then, as a retaliatory measure, the US could therefore divest the EU or this Member State from the status of a "covered country". This withdrawal of protection, however, must be explicitly ordered by the Attorney General after consultation with other authorities. Moreover, non-US persons may only receive protections under the Privacy Act, if their country first "effectively shares information with the United States for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses."¹⁰⁴⁴ Some non-US persons might therefore not be eligible for protection under the Privacy Act, until the country of their citizenship first transfers information to the US. Since the JR Act regulates the protection of foreigners, the involvement of a supranational agency from the country concerned, for example the EU, or an arbitration board might have been a better alternative to the mechanism used. Claims for compensation because of decisions that were made based on incorrect data are also excluded. Furthermore, there is the possibility for the competent judge to keep records secret and to restrain information to non-US citizens who request information, why a complaint has been

¹⁰⁴¹ European Commission. *Commission statement regarding the EU/US Agreement on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses ("Umbrella Agreement")*, OJ L 25, (31 January 2017).

¹⁰⁴² EPIC. (16 September 2015). *Re: Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015*. <https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf>.

¹⁰⁴³ US Department of Justice. (28 December 2022). *Judicial Redress Act of 2015 & U.S.-EU Data Protection and Privacy Agreement*. <https://www.justice.gov/opcl/judicial-redress-act-2015>.

¹⁰⁴⁴ H.R. 1428(d)(1)(B)

refused. This conflicts with the rights of data subjects, as provided in the LED. The JR Act also provides for far-reaching exceptions that can also be applicable to secret services (5 U.S.C. § 552a (j), (k)). Incidentally, enforcing their rights is also difficult for US citizens. Access to personal data by intelligence authorities can be challenged, for example, with an action for an injunction or under constitutional law. For this, however, a specific concern must be proven. Various lawsuits have already failed because of this hurdle.¹⁰⁴⁵ Due to the third-party doctrine, according to which data are not protected under the Fourth Amendment of the US constitution, if they have been previously disclosed to a third party, enforcement would be difficult anyway.

1.2.7. Cloud Act

On 23 March 2018, the Cloud Act entered into force. It is a supplement to the SCA. As the SCA, which itself was reformed by the ECPA, didn't anticipate the rise of cloud technology, the provisions of the SCA were adapted to the technological development through the Cloud Act.¹⁰⁴⁶ This Act was enacted to address scenarios where the SCA authorizes the US government to collect data from an entity doing business in the US and the data are stored outside the US. The Cloud Act was preceded by two legislative initiatives with a similar aim: the "Law Enforcement Access to Data Stored Abroad Act" (LEADS Act)¹⁰⁴⁷ and the International Communications Privacy Act (ICPA)¹⁰⁴⁸. Both intended to update legislation for law enforcement access to data stored abroad. Although both were finally no longer pursued, they show the efforts of US Congress and US Senate since 2016 to eliminate legal uncertainties, albeit primarily only for US authorities.

Since many providers of communications services store data in cloud systems and thus often outside the US, this has led to a legal dispute over the scope of the SCA in two significant cases. On the plaintiff side were Microsoft and Google¹⁰⁴⁹. Both companies were ordered to produce communications content of their users under a search warrant. Another common feature of the two legal disputes was the fact that the personal data requested was located on servers outside the US. As an example, we will take a closer look at the "*Microsoft Ireland*" case¹⁰⁵⁰, in which Microsoft did not comply with the order and was sentenced on 25 April 2014 to disclose the data.¹⁰⁵¹ The Court of Appeal (Second Circuit), however, overturned the search warrant on 14 July 2016, concluding that the US Congress did not intend the SCA's warrant provisions to apply extraterritorially and that the SCA does not authorize a US court to issue and enforce a SCA warrant against a US-based service provider for the contents of a customer's electronic communications stored on servers located outside the US. The Court of Appeal also rejected the complaint of the US government in January 2017.¹⁰⁵² After a "petition" (*writ of certiorari*) filed by the US Department of Justice against the judgment, the final decision by the US Supreme Court was expected. Meanwhile, however, the US government withdraw its original warrant and obtained a new warrant for the same

¹⁰⁴⁵ USA. *Obama v. Klayman*, Court of Appeals, D. C. Circuit, Case 14-5004, (28 August 2015). //US Supreme Court, *Clapper v. Amnesty International USA*, 26 February 2013, Case No. 11-1025

¹⁰⁴⁶ the SCA, which is integrated in the ECPA, had been interpreted over the years to cover the processing of personal data connected to data subjects' Internet transactions.

¹⁰⁴⁷ USA. *The LEADS Act*, S.512, H.R. 1174.

¹⁰⁴⁸ USA. *International Communications Privacy Act*, 115th Congress (2017-2018), S.1671.

¹⁰⁴⁹ USA. *In re Search Warrant No. 16-960-M-01 to Google*, US District Court, E.D. Pennsylvania, 232 F. Supp.3d 708, (3 February 2017).

¹⁰⁵⁰ USA. *Microsoft Corporation v. United States of America*, 2d Cir., Case No. 14-2985, (14 July 2016).

¹⁰⁵¹ USA. District Court Southern District of New York, 13 Mag. 2814, (25 April 2014).

¹⁰⁵² USA. *Microsoft Corporation v. United States of America*, 2d Cir., Case No. 14-2985, (14 July 2016).

objective in March 2019. The latter already fell under the new rules of the Cloud Act and “had the immediate effect of mooted the ongoing U.S. v. Microsoft litigation”.¹⁰⁵³

Both cases caused considerable irritation across Europe. Access by US authorities to data stored in the EU is usually guaranteed by means of a MLAT with the involvement of the respective governmental bodies. Without the participation of the Irish government and thus without observing the existing international agreements, a quasi “extraterritorial search warrant” was possible. The Commission addressed this consequence also in its European Data Strategy:

While third country legislations like the U.S. CLOUD Act are based on public policy reasons such as law enforcement access to data for criminal investigations, the application of foreign jurisdictions’ legislation raises legitimate concerns for European businesses, citizens and public authorities over legal uncertainty and compliance with applicable EU law, such as data protection rules. The EU is acting to mitigate such concerns through mutually beneficial international cooperation, such as the proposed EU-U.S. Agreement to facilitate cross border access to electronic evidence, alleviating the risk of conflict of laws and establishing clear safeguards for the data of EU citizens and companies. The EU is also working at the multilateral level, including in the context of the Council of Europe, to develop common rules on access to electronic evidence, based on a high level of protection of fundamental and procedural rights.¹⁰⁵⁴

At this point, it should not be forgotten that the Umbrella Agreement does not apply to all data accesses but is only a special tool to regulate the transatlantic authority-to-authority transfer. This was again clarified through the *Microsoft Ireland* case. If the Umbrella Agreement would have been in force at the time of the *Microsoft Ireland* case, it would not have been applicable to the issue in question because the *Microsoft Ireland* case did not concern a matter of data transfer between public bodies but of a public body accessing data stored on a company’s servers abroad. The data subject would still have had the right to defend himself in national courts against such a search, but it would not have been able to rely on the Umbrella Agreement.

In principle, the so-called “presumption against extraterritoriality”¹⁰⁵⁵ applies in the US. According to this presumption, the regulatory scope of US laws ends in doubt at the country’s own borders, unless a different intention of the legislator is discernible. To interpret this intention, a court first examines whether the statute in question gives a clear, affirmative indication that it applies extraterritorially. If this is not the case, the court must clarify in a second step which behavior is “territorially” according to the law; the court does this by looking at the statute’s “focus” (therefore also called “focus test”).

Against this background, a US Court of Appeals found that 18 U.S.C. § 2703 only concerns data that are stored on servers in the US because a different interpretation would violate this presumption.¹⁰⁵⁶ The court found further that this presumption has not been refuted and that there was no evidence that the US Congress intended that the SCA should collect data stored by a service provider abroad.¹⁰⁵⁷ Adherence to the

¹⁰⁵³ Artzt, M. [Matthias] and Delacruz, W. [Walter]. (29 January 2019). *How to comply with both the GDPR and the CLOUD Act*. <https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act>.

¹⁰⁵⁴ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 9.

¹⁰⁵⁵ “Thus, unless there is the affirmative intention of the Congress clearly expressed to give a statute extraterritorial effect, we must presume it is primarily concerned with domestic conditions. [...] When a statute gives no clear indication of an extraterritorial application, it has none.” See USA. *Morrison v. National Australia Bank*, Supreme Court, 561 U.S. 247, (24 June 2010). P. 255.

¹⁰⁵⁶ USA. *Microsoft Corp. v. United States*, 2nd Cir. 2016, 829 F.3d 197, (14 July 2016). P. 222.

¹⁰⁵⁷ USA. *Microsoft Corp. v. United States*, 2nd Cir. 2016, 829 F.3d 197, (14 July 2016). P. 216.

presumption against extraterritoriality could be made difficult by a 2016 amendment to US criminal procedure law. This amendment¹⁰⁵⁸, which is explicitly declared to be extraterritorial, allows search warrants to be issued even in the case of electronically stored data “where the media or information has been concealed through technological means”. This does not exclude the possibility that data are located outside the US. Google’s data storage practice could well be seen as such technological means, which prevents the assignment to a certain jurisdiction. Such a classification could give the investigating authorities the opportunity to seize data located on Google’s servers by remote access. The US Court of Appeals found also that the focus of 18 U.S.C. § 2703 was to protect the privacy interests of users of electronic communications.¹⁰⁵⁹ In the Microsoft decision, this result of the focus test ultimately led the court to assume a violation of the presumption against extraterritoriality. As the execution of the search warrant took place outside US territory, an access to data stored on foreign servers would involve an impermissible extraterritorial application regardless of any other conduct that occurred on US territory.

18 U.S.C. § 2713 now provides that the obligation to comply with search warrant requirements applies “regardless of whether such communication, record, or other information is located within or outside of the United States”. The Cloud Act therefore explicitly regulates extraterritorial application. The Act applies to the contents of electronic communications, documents stored in the cloud, and to certain types of transmission and account information. Providers of such communications are now obliged to “comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control”, 18 U.S.C. § 2713.

The prerequisite is that the communications service provider is subject to US jurisdiction. For this purpose, “minimal contacts” to the US are sufficient, which can exist even without the service provider’s headquarters or branch office in the US. Therefore, whether a US-based provider must produce those data, depends on the organizational structure of the provider, including the relationship of the parent of the MNE to its offshore affiliates.¹⁰⁶⁰ This structure could be such that no data storage in an EU affiliate, no EU-US-business and no data access from the non-EU corporate parents is given; then the Cloud Act would not be applicable. If, however, an offshore entity (e.g., within the EU) of this MNE does not operate independently of its corporate parents in the US, the Cloud Act applies.

The requesting authority must prove facts if there is suspicion that the requested data are important for the criminal proceedings initiated. If the production of the data is based on a subpoena or a court order, the data subject must be informed by the US authority, whereby the duty to provide information is subject to the requirements of 18 U.S.C. § 2705 and can temporarily be suspended. If the production request is based on a search warrant, no information towards the data subject is required. 18 U.S.C. § 2703(h)(2) also introduced legal remedies for providers. A provider can lodge an appeal with a competent court to challenge the warrant. Under certain conditions, the provider can claim the request to be changed or declared ineffective. The court then, after hearing the government side, balances reasons, using the following guidelines:

¹⁰⁵⁸ Rule 41(b)(6) [A] of the US Federal Rules of Criminal Procedure

¹⁰⁵⁹ USA. *Microsoft Corp. v. United States*, 2nd Cir. 2016, 829 F.3d 197, (14 July 2016). P. 212.

¹⁰⁶⁰ Artzt, M. [Matthias] and Delacruz, W. [Walter]. (29 January 2019). *How to comply with both the GDPR and the CLOUD Act*. <https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act>.

- (i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;
- (ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and
- (iii) the customer or subscriber is not a United States person and does not reside in the United States.

Criterion (ii) is specified by the so-called “comity analysis”, based on eight criteria to be considered:

- (3) COMITY ANALYSIS. – For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate –
- (A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;
 - (B) the interests of the qualifying foreign government in preventing any prohibited disclosure;
 - (C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;
 - (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer’s connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer’s connection to the foreign authority’s country;
 - (E) the nature and extent of the provider’s ties to and presence in the United States;
 - (F) the importance to the investigation of the information required to be disclosed;
 - (G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and
 - (H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

The Cloud Act introduced the concept of a “qualified foreign government”, which is a country with which the US has an executive agreement and which, at least in principle, guarantees similar safeguards as the Cloud Act, and reciprocity. Also, this “qualified foreign government” must refrain from prosecuting US citizens for obtaining data. Thus, a provider’s complaint can only succeed if the provider is subject to the law of a qualifying State’s foreign government. This concept could put pressure on other countries to enter into executive agreements with the US, combined with the need for those countries to introduce a similar comity analysis by law. This could happen, for example, through the E-Evidence Regulation in the EU, which is also based on the principle that (US) investigators can approach the provider directly and the provider can then lodge a complaint. It is noteworthy – although both were declared invalid – that “the earlier EU-U.S. Safe Harbor and Privacy Shield agreements did not include a U.S. finding about European privacy protections, although the 2018 CLOUD Act similarly requires a U.S. attorney general finding before European or other countries can have access to certain types of data”¹⁰⁶¹.

¹⁰⁶¹ Swire, P. [Peter]. (18 July 2023). *A guide to the attorney general’s finding of ‘reciprocal’ privacy protections in EU*. <https://iapp.org/news/a/a-guide-to-the-attorney-generals-finding-of-reciprocal-privacy-protections-in-eu/>.

On 10 July 2019, EDPB and EDPS replied to LIBE with a first legal analysis of the impact of the Cloud Act on the European legal framework for the protection of personal data.¹⁰⁶² They concluded that the required level of protection for data subjects in the EU and legal certainty for companies can only be effectively guaranteed by means of a data protection compliant international agreement with strict procedural and substantive fundamental rights guarantees. According to applicable law, such a data transfer in accordance with the requirements of the GDPR would only be possible within narrow limits. Such processing would be unlawful unless a) an appropriate order from a US court, based on an international agreement, is recognized, or made enforceable, and could therefore be a legal obligation in accordance with Art. 6(1)(b) and (c) GDPR, or there are circumstances that require a data processing to protect the vital interests of the data subject based on Arts. 6(1)(d), 49(1)(f) GDPR. In the absence of a corresponding legal framework or another legal basis in accordance with the GDPR, providers that are subject to EU law do not have a sufficient legal basis for the transfer of personal data to US agencies in the context of such orders. The EDPB not only reaffirmed its position formulated in the guidelines on Art. 49 GDPR but made also particular reference to the opinion of the European Commission.¹⁰⁶³ In this context, the WP29 had already reaffirmed that foreign public bodies may only access data in Europe with the involvement of public authorities, orders must not be made directly to European companies themselves.¹⁰⁶⁴

It is also noticeable that the procedural path of these orders must be based on an international agreement, such as a MLAT between the requesting third country and the Union or a Member State, as prescribed in Art. 48 GDPR. The Cloud Act does not mention the MLAT procedure. Simple administrative agreements are difficult to interpret falling below Art. 48 GDPR. Cloud providers affected could try to justify their cooperation with the US judiciary with Art. 49(1)(e) GDPR. This justification is doubtful because the comity analysis in the Cloud Act intervenes before transfer. In addition, the Cloud Act uses the term “United States person”, whilst the GDPR “data subject” – regardless of nationality or place of residence. For this reason, the Cloud Act and the GDPR do not seem to fit together. However, contrary to other arguments put forward by US authorities, compliance with EU data protection law does not mean that an order by US authorities to data access is generally excluded. There is still the possibility of a MLAT, which has been carefully negotiated by an international law treaty and considers the interests of both Parties.¹⁰⁶⁵

1.2.8. Initiatives for a Federal Data Protection Law

Since the end of 2018, the US government discusses a legislative proposal to ensure a nationally uniform level of data protection. Department of Commerce officials therefore also met with representatives from Meta and Google, providers such as AT&T and Comcast, and consumer advocates for a multi-stakeholder approach.¹⁰⁶⁶

¹⁰⁶² EDPB. *Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection*, OUT2019-0007, (10 July 2019).

¹⁰⁶³ EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018).

¹⁰⁶⁴ WP29. *Joint statement of the European Data Protection Authorities assembled in the Article 29 Working Party*, WP 227, (26 November 2014).

¹⁰⁶⁵ The US has such MLATs with about half the countries in the world, including Ireland. The EU-US MLAT (EU. *Agreement on mutual legal assistance between the European Union and the USA*, OJ L 181, 34–40, (19 July 2003)), which was signed in 2003, complements those bilateral agreements.

¹⁰⁶⁶ Romm, T. [Tony]. The Trump administration is talking to Facebook and Google about potential rules for online privacy. *The Washington Post*. <https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/>. // Shepardson, D. [David]. (27 July 2018). Trump administration working on consumer data privacy policy. *Reuters*. <https://www.reuters.com/article/us-usa-internet-privacy-idINKBN1KH2MK>. // Kurzer, R. [Robin]. (13 August 2018). *The United States finally starts to talk about data privacy legislation*. <https://martechtoday.com/the-united-states-finally-starts-to-talk-about-data-privacy-legislation-219299>.

In 2021 alone, there were dozens of bills relating to data protection introduced by US Congress, but “while most of these bills addressed specific privacy issues, such as rules for contact tracing apps, vaccine passports, or social media, a handful of bills propose a broader federal privacy framework.”¹⁰⁶⁷ This work can therefore only cover key bills related with the scope of this thesis.

One of the first legislative initiatives was the “Online Privacy Act of 2019”¹⁰⁶⁸ (OPA). The initiative proposed to set up a new federal agency (“Digital Privacy Agency”) to monitor technology companies. Users of online platforms should also be granted the right to access, correct, delete or transfer their data at any time. It would essentially bring those rights guaranteed by the “California Consumer Privacy Act” (CCPA)¹⁰⁶⁹ to non-California residents, as well as additional user rights, such as the right to choose how long data can be kept and opt-in consent for the use of data for A.I. algorithms. The initiative did not receive a vote in congress and was referred to the Subcommittee on Antitrust, Commercial, and Administrative Law on 18 December 2019.

In December 2019, the “Consumer Online Privacy Rights Act”¹⁰⁷⁰ (COPRA) was introduced to provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement. Numerous rules within COPRA suggest that the GDPR also served as a blueprint. Among other things, rules are also provided which are intended to regulate the access to and transparency of the personal data processed. Data subjects should receive detailed and clear information about the processing and the alleged disclosure of their data (Sec. 102), similar to Arts. 13 and 14 GDPR. As a result, data subjects should be given the right to control their data (Sec. 105), in particular to give them the opportunity to prevent their personal data from onward transfer to unknown third Parties. In addition, the draft law contains the right to delete or correct personal data (Sec. 104) and the right to data portability (Sec. 110), further similarities to the rules in the GDPR. The Act has been referred to the Committee on Commerce, Science, and Transportation on 3 December 2019.

The “Data Protection Act of 2020”¹⁰⁷¹ was introduced in February 2020. One main aim of this initiative was the creation of a Federal Data Protection Agency in the US. The Data Protection Agency would stand alongside the FTC and exercise its powers in the area of “Federal privacy law”. The draft first defines the content of a right to privacy that must be guaranteed by the data protection agency: “The right to privacy protects the individual against intrusions into seclusion, protects individual autonomy, safeguards fair processing of data that pertains to the individual, advances the just processing of data, and contributes to respect for individual civil rights and fundamental freedoms.” (Sec. 2 (3)). The social importance of privacy is also emphasized (Sec. 2 (4)). Accordingly, the purpose of the authority is summarized: “The Agency shall seek to protect individuals’ privacy and limit the collection, disclosure, processing and misuse of individuals’ personal data by covered entities [...]” (Sec. 6 (a)). In addition to protecting the right to privacy, the agency would be given the responsibilities of providing advice on data protection issues, providing information to the public, promoting the implementation of appropriate data protection practices in the public and private sectors, and representing the US in international forums. In addition, the implementation of the requirements of 5 U.S. § 552 should be monitored by federal authorities. This article is attached to the

¹⁰⁶⁷ Castro, D. [Daniel] and Dascoli, L. [Luke] and Diebold, G. [Gillian]. (24 January 2022). *The Looming Cost of a Patchwork of State Privacy Laws*. <https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws>.

¹⁰⁶⁸ USA. *Online Privacy Act of 2019*, 116th Congress (2019-2020), H.R. 4978.

¹⁰⁶⁹ California State. *California Consumer Privacy Act 2018*, Cal. Legis. Serv. Ch. 55 (A.B. 375). // All references to the “CCPA” are to Section 3, Title 1.81.5 of the CCPA, added to Part 4 of Division 3 of the California Civil Code.

¹⁰⁷⁰ USA. *Consumer Online Privacy Rights Act*, 116th Congress (2019-2020), S.2968.

¹⁰⁷¹ USA. *Data Protection Act of 2020*, 116th Congress (2019-2020), S.3300.

“Freedom of Information Act” (FOIA)¹⁰⁷² and deals with the handling of personal data of US citizens and permanent residents by federal authorities. The Federal Data Protection Agency to be created would also have a consumer protection function to ensure adequate contractual terms in the market, including the ban on “pay-for-privacy” and “take-it-or-leave-it” (Sec. 6 (b) (7)). It would also serve as a point of contact for consumer complaints. The Federal Data Protection Agency would be designed as an independent executive body and chaired by a director appointed by the POTUS. His/her appointment would have to be confirmed by the US Senate and term of office expected to be five years. At the same time, the law would bring with it a series of structural fundamental decisions on data protection in the US, which are based on the European data protection regime. The rules would cover every person who processes personal data. “Personal or household activity” are excluded. In addition to “personal data”, the law also knows so-called “high-risk data practices”. This includes e.g., profiling, the processing of sensitive data, the systematic monitoring of publicly available data, decisions about access to services and products, the processing of biometric data to identify a person, the use of personal data of children and other vulnerable groups and the use of personal data for marketing purposes. The term “sensitive data” is defined based on the special categories of personal data in European data protection law. Known data protection principles, such as Privacy by Design and data minimization, are also included (Sec. 6 (b) (8)). The draft foresees special requirements in Sec. 8 for so-called “very large covered entities”. Those are data controller who have annual sales more than USD 25 million, handle the data of more than 50.000 people, households, or devices and generate 50% or more of their income from the sale of personal data. Fines are provided as judicial daily rates that can be imposed if an infringement is not remedied. Unfortunately, the draft also contains numerous open wordings, which therefore requires interpretation, and should attract criticism like against the CCPA. The Federal Data Protection Agency itself would be responsible for specifying this wording. The States would have the option to enact or maintain their own data protection laws as long as they meet the minimum standard set by the Data Protection Act of 2020. The Act has been referred to the Committee on Commerce, Science, and Transportation on 13 February 2020.

In July 2020 the draft “Data Accountability and Transparency Act 2020”¹⁰⁷³ was published. Its focus lies on consent as the central basis for the processing of personal data. Strict and clear processing principles instead of relying on consent would also shift the focus of privacy statements from consent to consumer information. The material part of the draft starts with a general prohibition: “A data aggregator shall not collect, use, or share, or cause to be collected, used, or shared any personal data, unless the data aggregator can demonstrate that such personal data is strictly necessary to carry out a permissible purpose under section 102.” A list of twelve exceptions is located there, the first entry of which corresponds to Art. 6(1)(b) GDPR. Among other things, processing is permitted “to detect or to respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity”. There is no provision for an equivalent to Art. 6(1)(f) GDPR. In addition, the draft contains a list of “unlawful data practices”, for example to “terminate, refuse to provide, degrade goods or services to, or otherwise retaliate against, a person that exercises the rights of the person under this Act.” (Sec. 103 (a) (2)). An independent SA (“Data Accountability and Transparency Agency”) based on the European model is planned to monitor the requirements of the bill. The draft includes a preemption clause, which means the bill would remain open to further tightening at the State law level. The Act has been referred to the House Committee on Energy and Commerce.

¹⁰⁷² 5 U.S.C. § 552

¹⁰⁷³ USA, Senate. *Data Accountability and Transparency Act 2020, Released as a Discussion Draft by Senator Sherrod Brown*, <https://www.banking.senate.gov/imo/media/doc/DATA2020%20One-Pager.pdf>

The “Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act” (Safe Data Act)¹⁰⁷⁴ is a conglomeration of three previously introduced legislative proposals: the draft of the “United States Consumer Data Privacy Act of 2019” (USCDPA)¹⁰⁷⁵, the “Filter Bubble Transparency Act”¹⁰⁷⁶ and the “Deceptive Experiences To Online Users Reduction Act”¹⁰⁷⁷. The Safe Data Act includes a definition of personal data like that of the GDPR. Aggregated data, de-identified data, employee data and publicly available information are excluded. Like the GDPR, the initiative also regulates “affirmative express consent”. The draft also relies on the obligation to inform and offers data subjects possibilities to control their data by establishing individual rights, derived from the CDPA. A right of revocation for consents, claims to data deletion and the principle of data minimization are also established. There are also provisions on transparency, the integrity of processing and data security, which also extend to the transparency of algorithms and rules against unfair and deceptive acts and practices relating to the manipulation of user interfaces. Nevertheless, the Safe Data does not entitle a regular person to enforce their rights. The section on corporate responsibility contains rules on the appointment of a data protection and data security officer, internal control of data protection and the protection of whistleblowers. The FTC would be called to seek a permanent injunction and other remedies in the case of violations and would be given more resources and powers to enforce. The initiative has been referred to the Committee on Commerce, Science, and Transportation.

The “Protecting Americans’ Data from Foreign Surveillance Act”¹⁰⁷⁸ aimed to foster national security with those to limit excessive trading of personal data.¹⁰⁷⁹ Under the bill, the US government would first draw up a list of countries to which data can be transferred. Providers based in another country would first have to apply for an export license before being allowed to process data from US citizens. In addition, citizens are to receive claims for damages if they suffer harm. Not only geopolitical opponents of the US could thus be excluded from the global data stream, as Johnny Ryan of the Irish Council on Civil Liberties (ICCL) warned.¹⁰⁸⁰ He feared that the delayed handling of privacy complaints with the Irish SA could result in Ireland being put on the list of unreliable countries. This would have enormous consequences: “Obtaining these licenses is difficult: these are the same restrictions that are applied to nuclear material”, Ryan warned in this open letter. To directly prevent such a scenario, the ICCL asked for a more consistent implementation of the GDPR. Senator Wyden justified his bill with the aim that

shady data brokers shouldn’t get rich selling Americans’ private data to foreign countries that could use it to threaten our national security. My bill would set up common sense rules for how and where sensitive data can be shared overseas, to make sure that foreign criminals and spies don’t get their hands on it. This legislation is another

¹⁰⁷⁴ USA, Senate. *Safe Data Act*, <https://www.commerce.senate.gov/services/files/BD190421-F67C-4E37-A25E-5D522B1053C7>.

¹⁰⁷⁵ Hunton Williams. *United States Consumer Data Privacy Act of 2019*. <https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf>

¹⁰⁷⁶ USA. *Filter Bubble Transparency Act*, 116th Congress, S.2763.

¹⁰⁷⁷ USA. *Deceptive Experiences To Online Users Reduction Act*, 116th Congress, S.1084.

¹⁰⁷⁸ USA, Senate. *Protecting Americans’ Data from Foreign Surveillance Act*, <https://www.wyden.senate.gov/imo/media/doc/Protecting%20Americans%20Data%20from%20Foreign%20Surveillance%20Act%20of%202021%20Bill%20Text.pdf>

¹⁰⁷⁹ Wyden, R. [Ron]. (2023). *The Protecting Americans’ Data From Foreign Surveillance Act – Onepager*. <https://www.wyden.senate.gov/imo/media/doc/Protecting%20Americans%20Data%20from%20Foreign%20Surveillance%20Act%20of%202021%20One%20Pager.pdf>.

¹⁰⁸⁰ Irish Council for Civil Liberties. (15 April 2021). *New economic risk: draft US Senate Bill and Ireland’s GDPR enforcement*. <https://www.iccl.ie/wp-content/uploads/2021/04/Letter.pdf>.

piece in a slate of bills I'm introducing this Congress to provide comprehensive protection for Americans' sensitive information.¹⁰⁸¹

While members of Congress have introduced multiple proposals, none have yet had widespread bipartisan support. This might change through the latest development in the US at federal stage, which has come to attention of the public on 3 June 2022 with a proposal for an "American Data Privacy and Protection Act" (ADPPA)¹⁰⁸², which was slightly amended¹⁰⁸³ on 20 July 2022 and is now eligible for a full US House of Representatives floor vote. US House and Senate leaders commented that

this bill strikes a meaningful balance on issues that are critical to moving comprehensive data privacy legislation through Congress, including the development of a uniform, national data privacy framework, the creation of a robust set of consumers' data privacy rights, and appropriate enforcement mechanisms. We believe strongly that this standard represents the best opportunity to pass a federal data privacy law in decades, and we look forward to continuing to work together to get this bill finalized and signed into law soon.¹⁰⁸⁴

Preemption and the private right of action were the major areas of concern in this draft proposal. According to Politico, a

bipartisan group of lawmakers have reached an agreement on two of the biggest points of contention in negotiations on a federal privacy bill. [...] The draft bill includes an agreement that the federal law will preempt most state laws — with some exceptions — and a limited private right of action allowing individuals to seek damages from a court for privacy violations.¹⁰⁸⁵

Public Knowledge Senior Policy Counsel Sara Collins stated that "you've seen a willingness to negotiate [on preemption] because really broad preemption does hit traditional areas of state control that I don't think a lot people actually wanted overturned at the state level, so there were going to have to be real considerations."¹⁰⁸⁶ Brookings Institution Tisch Distinguished Visiting Fellow Cameron Kerry said that this bipartisan agreement "is an even bigger deal where it includes civil rights protection in the use of personal data that key civil rights organizations have received favorably, and a private right of action."¹⁰⁸⁷ The private right of action would start two years after ADPPA goes into effect. Individuals would need to first notify their State attorney general and the FTC of their intent to bring suit, and if one of those agencies decides to initiate an action, individuals wouldn't be allowed to file their own lawsuit. Through the last amendment to the proposed ADPPA in July 2022, a small business exception to the private right of action was added to Sec. 203, determining that it does not apply to any claim against a covered entity that has less than USD 25,000,000 per year in revenue, collects,

¹⁰⁸¹ Wyden, R. [Ron]. (15 April 2021). *Wyden Releases Draft Legislation to Protect Americans' Personal Data From Hostile Foreign Governments*. <https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments>.

¹⁰⁸² USA. *American Data Privacy and Protection Act*, H.R. 8152 (117th), (21 June 2022).

¹⁰⁸³ USA. *American Data Privacy and Protection Act*, H.R. 8152 (117th), (21 July 2022).

¹⁰⁸⁴ USA, Senate Committee on Commerce, Science, and Transportation. (3 June 2022). *House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill*. <https://www.commerce.senate.gov/2022/6/house-and-senate-leaders-release-bipartisan-discussion-draft-of-comprehensive-data-privacy-bill>.

¹⁰⁸⁵ Kern, R. [Rebecca]. (1 June 2022). Lawmakers reach bipartisan compromise on privacy bill with preemption, right to sue. *Politico*. <https://subscriber.politicopro.com/article/2022/06/lawmakers-reach-bipartisan-compromise-on-privacy-bill-with-preemption-right-to-sue-00036563?source=email>.

¹⁰⁸⁶ Duball, J. [Joseph]. (2 June 2022). *US lawmakers closing in on bipartisan privacy framework*. <https://iapp.org/news/a/us-lawmakers-closing-in-on-bipartisan-privacy-framework>.

¹⁰⁸⁷ Duball, J. [Joseph]. (6 June 2022). *US lawmakers unveil bipartisan American Data Privacy and Protection Act*. <https://iapp.org/news/a/congress-unveils-american-data-privacy-and-protection-act>.

processes, or transfers the covered data of fewer than 50,000 individuals, and derives less than 50 percent of its revenue from transferring covered data. Despite this significant reduction in the scope of this right compared to the first draft, there is still opposition against a private right of action as such. Castro / Dascoli / Diebold found that “congress should avoid creating a private right of action that would open a floodgate of expensive, and unnecessary, lawsuits against organizations subject to the new law”¹⁰⁸⁸ and the US Chamber of Commerce commented that “a national data protection law including a private right of action would encourage an influx of abusive class-action lawsuits, create further confusion regarding enforcement of blanket privacy rights, harm small businesses, and hinder data-driven innovation.”¹⁰⁸⁹ The amended ADPPA proposal, inter alia, enlarged the definition of sensitive covered data, expanded the employee data carveout, expressly included the CCPA as having the power to enforce the ADPPA in California, included new permissible purposes for reasonably, necessary and proportionate covered data use, and included technical changes to the definitions for “covered entity” and “service provider”, which now makes clear that entities acting on behalf of government entities to provide services using covered data remain subject to ADPPA.

As the Congressional Research Service commented, “ADPPA is, in many ways, similar to a number of other consumer privacy bills introduced in the 116th and 117th [until 3 January 2023] Congresses”¹⁰⁹⁰. Therefore, different elements of these federal legislative instruments were compared: ADPPA, COPRA, The Data Care Act of 2021¹⁰⁹¹, OPA, and the Control Our Data Act (CODA)¹⁰⁹².

¹⁰⁸⁸ Castro, D. [Daniel] and Dascoli, L. [Luke] and Diebold, G. [Gillian]. (24 January 2022). *The Looming Cost of a Patchwork of State Privacy Laws*. <https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws>.

¹⁰⁸⁹ USA, Chamber of Commerce. (31 May 2022). *U.S. Chamber Warns It Will Oppose Any Privacy Legislation That Creates a Blanket Private Right of Action*. <https://www.uschamber.com/technology/data-privacy/u-s-chamber-warns-it-will-oppose-any-privacy-legislation-that-creates-a-blanket-private-right-of-action>.

¹⁰⁹⁰ USA, Congressional Research Service. *Overview of the American Data Privacy and Protection Act, H.R. 8152, LSB10776*, (31 August 2022). P. 1.

¹⁰⁹¹ USA. *Data Care Act of 2021*, 117th Congress (2021-2022), S.919.

¹⁰⁹² Eggerton, J. [Jon]. (3 November 2021). *House Republicans Tag Team on Privacy Bill Draft*. <https://www.mediainstitute.org/2021/11/03/house-republicans-tag-team-on-privacy-bill-draft/>

Table 1. Comparison of Enforcement Mechanisms and Preemption

	ADPPA	COPRA	Data Care Act	OPA	CODA
Enforcement					
Federal Agency Enforcement	FTC (§ 401)	FTC (§ 301(a))	FTC (§ 4(a))	New Digital Privacy Agency (Tits. III and IV)	FTC (§ 113(a))
State Attorneys General	Yes (§ 402)	Yes (§ 301(b))	Yes (§ 4(b))	Yes (§ 404)	Yes (§ 113(b))
Private Right of Action	Yes, with two-year phase-in (§ 403)	Yes (§ 301(c))	Silent	Yes (§ 405)	No (§ 113(f))
State Law Preemption	Yes, with exceptions (§ 404(b))	Yes, if state laws afford less protection ((§ 302(c))	No (§ 6(1))	Silent	Yes (§ 112(a))

Table 2. Comparison of Rights and Obligations

	ADPPA	COPRA	Data Care Act	OPA	CODA
Individual Rights					
Access	§ 203(a)(1)	§ 102(a)	Silent	§ 101	§ 102(c)(1)(B)
Correction	§ 203(a)(2)	§ 104	Silent	§ 102	§ 102(c)(1)(C)
Deletion	§ 203(a)(3)	§ 103	Silent	§ 103	§ 102(c)(1)(D)
Opt Out	§ 204	§ 105(b)	Silent	§ 208(b)	§ 102(c)(1)(E)
Portability	§ 203(a)(4)	§ 105(a)	Silent	§ 104	Silent
Obligations					
Notice	§ 202(e)	§ 102(b)	Silent	§ 210	§ 102(b)
Affirmative Consent for Sensitive Info.	§ 102(a)(3)(A)	§ 105(c)	Silent	§ 210	§ 103
Privacy Policy	§ 202(a)	§ 102(b)	Silent	§ 211	§ 102(a)
Minimization	§ 101	§ 106	Silent	§§ 201-202	§§ 104-105
Data Security	§ 208	§ 107	§ 3(b)(1)(A)	§ 212	§ 109
Breach Notices	Silent	Silent	§ 3(b)(1)(B)	§ 213	Silent

Source: US Congressional Research Service, "Overview of the American Data Privacy and Protection Act, H.R. 8152"¹⁰⁹³

A more detailed analysis especially regarding principles, and essential guarantees provided in the proposed ADPPA, will be done in Chapter IX Section III.2 and Chapter IX Section III.3.

It can be summarized at this point that the various initiatives at the US federal law level have a wide variety of regulatory objectives:

¹⁰⁹³ US Congressional Research Service. *Overview of the American Data Privacy and Protection Act, H.R. 8152*, LSB10776, (31 August 2022). P. 3–4.

Initiative	Main objectives
Online Privacy Act of 2019	New Federal Data Protection Agency, CCPA-like data subject rights
COPRA	Data subjects' rights alike GDPR
Data Protection Act of 2020	New Federal Data Protection Agency, Scoping of the Right to Privacy, some Data Protection Principles, especially Privacy by Design
Data Accountability and Transparency Act 2020	Consent, Default position with general prohibition, together with 12 exceptions
Safe Data Act	Requirement for data protection- and data security officer, FTC with more resources for enforcement, some Data Protection Principles
Protecting Americans' Data from Foreign Surveillance Act	National security focus, substantially limit the disclosure of US. citizens' personal data abroad
American Data Privacy and Protection Act	First comprehensive federal data protection proposal to gain bipartisan, bicameral support. Includes limited preemption and limited private right of action.

2. Selected State legislation

Several US States proposed data protection related bills. At least 38 States introduced more than 160 bills until the end of 2021.¹⁰⁹⁴ However, a distinction between “comprehensive” and other approaches at State level is necessary. Only those bills on State level are to be examined which are intended to represent “comprehensive” approaches to protect personal data. “Comprehensive” is hereby to be understood as “similar to the CCPA, i.e., broadly regulating the collection, use and disclosure of personal information and providing an express set of consumer rights with regard to collected data, such as the right to access, correct and delete personal information collected by businesses”.¹⁰⁹⁵ Industry-, information-specific, or narrowly scoped bills¹⁰⁹⁶ are not to be considered, unless they supplement comprehensive State law at specific points or create a comprehensive structure for a whole industry that is of central importance for transborder data flow (e.g., cloud provider).

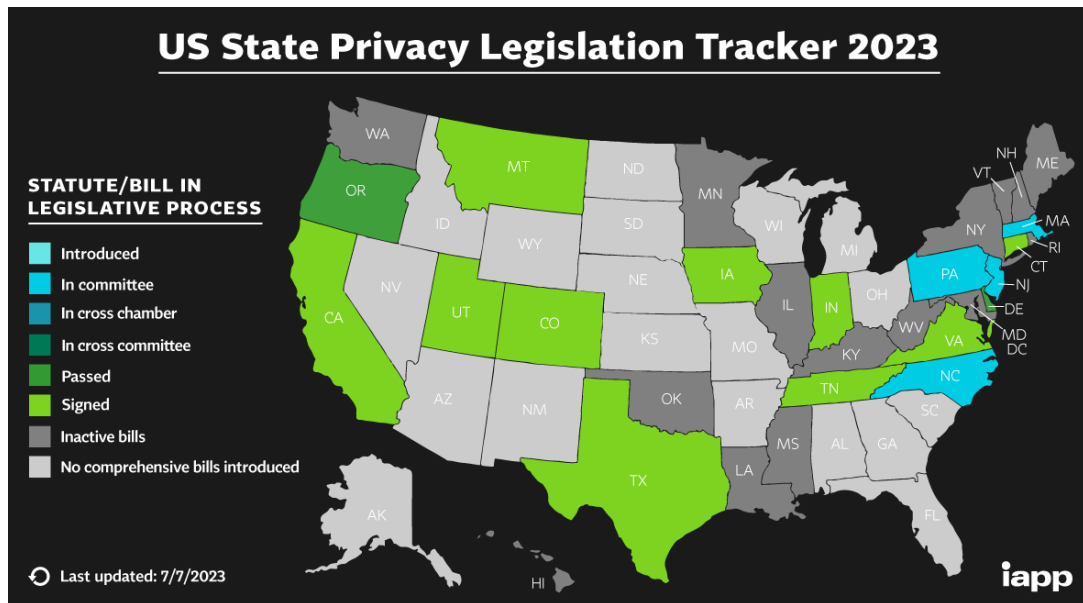
The California State is of particular economic importance for the US and, as the home of the so-called “Silicon Valley” (market-relevant companies such as Apple, Meta and Google are based there), occupies an outstanding position for the global information economy. California can therefore significantly influence the digital economy with its legislation. Due to the associated importance of this State, its laws are of the greatest interest for this Section II.2. of Chapter III.

The level for data protection bills has been increasing continuously, as the following graphic highlights.

¹⁰⁹⁴ Greenberg, P. [Pam]. (27 December 2021). *2021 Consumer Data Privacy Legislation*. <https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx>.

¹⁰⁹⁵ Greenberg, P. [Pam]. (27 December 2021). *2021 Consumer Data Privacy Legislation*. <https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx>.

¹⁰⁹⁶ E.g., Missouri has eBook privacy rules, and the Illinois Biometric Information Privacy Act gives people rights over their biometric personal data. While both Acts are “intensive” regulations in their specific field, they are not “extensive” enough into cover an at least significant part of the totality of all regulatory subjects relevant for a comprehensive protection of data protection rights.



Source: Desai, A. [Anokhy], "US State Privacy Legislation Tracker 2023"¹⁰⁹⁸

The "California Online Privacy Protection Act" (CalOPPA)¹⁰⁹⁹ is codified in California's Business and Professions Code Sec. 22575 - 22579. Due to the many sources that refer to CCPA and COPRA, it has been somewhat forgotten that there's already been one extensive law in place in California since 2004. Sec. 22575 begins by ascertaining the scope of the Act: "An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service [...]". CalOPPA therefore claims potentially global reach by linking to consumers "residing" within its territory, instead of those having "citizenship". This criterion of residence and the double domestic link can prevent unwanted random results and ensure a significant connection to the domestic market. Sec. 22576 also opens the scope of application if a commercial offer is targeted to persons with permanent residence in California, which can be interpreted as a link to the principle of impact, comparable with Art. 3(2)(a) GDPR. Sec. 22575(a) also sets an obligation for operators of a commercial website or an online service (service provider) to provide the user within the scope of a commercial website or a comparable online service (e.g., apps) with an easily accessible privacy policy. It should serve to provide the consumer with comprehensive information, for example by informing which categories of personal data are collected and, if necessary, which third Parties use the service to collect personal data.

Effective 1 January 2015, the California Business and Professions Code has been expanded to protect the online privacy of children and teenagers under 18 who live in California ("Privacy Rights for California Minors in the Digital World").¹¹⁰⁰ The primary aim was not to create a functioning information market and to educate consumers, but rather to protect minors living in California. This law applies to all Internet services unrelated to the country of the company's seat, if they are aimed at minors in California. Like the one in CalOPPA, this scope of application can be interpreted as a link to the principle of impact. In contrast to CalOPPA and COPPA, nevertheless, non-commercial offers are also in scope. The reason for the elevation of extraterritorial sovereignty in this new

¹⁰⁹⁸ Desai, A. [Anokhy]. (7 July 2023). *US State Privacy Legislation Tracker*. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker>.

¹⁰⁹⁹ California State. *California Online Privacy Protection Act of 2003, as amended by A.B. 370*, California Business & Professions Code Sec. 22575 - 22579 (2004), (11 January 2014).

¹¹⁰⁰ California State. *California Senate Bill no. 568 to add Chapter 22.1 (Sec. 22580 - 22582) to Division 8 of the Business and Professions Code*, (22 February 2013).

Section is, on the one hand, the need for the protection of children who cannot yet assess the scope of their actions in the online world and, on the other hand, the limitless nature of the Internet. This law obliges SPs to enable their underage users to delete content and information online, which includes, among other things, contributions to social networks. Herewith, a “right to erasure” was introduced.

The CCPA entered into force on 1 January 2020 and is enforceable since 1 July 2020. The law protects California residents and applies to organizations that are doing business in California. It does not require organizations to have a physical presence in California. The law can therefore apply to companies who target consumers in the California market. Thus, companies outside California – and also those outside the US –, which offer goods or services over the Internet targeted to California, can fall below the scope of the CCPA. Companies are only exempted from the scope if they started processing the personal data at a point in time when the consumer was outside California, no part of the sale or transfer of the personal data took place in California and no personal data was sold collected by the consumer at a time when he was in California (Section 1798.145 (a) (6)). The law applies to companies that have a gross annual revenue of more than USD 25 million, generate 50% or more of their annual revenue from the sale of consumer personal data, or receive or pass on personal data of more than 50.000 consumers annually for commercial purposes (Section 1798.140 (c) (1) (A) - (C)).

CCPA mainly concerns the consumer protection area. The GDPR, on the other hand, contains comprehensive guidelines regarding compliance and correct implementation of data protection, including enforcement. CCPA does not contain information on the appointment of a DPO. In CCPA, children between the ages of 13 and 16 must explicitly give their consent. In contrast to the GDPR, there is no need to display a so-called “cookie banner” which would offer the possibility to give or to decline consent before using a website. However, since the CCPA also classifies cookies (first-party and third-party cookies) as personal data, consumers can use the opt-out option to prevent advertisers from displaying product placements by using tracking measures. The CCPA only requires parental consent for personal data sales.

Both CCPA and GDPR focus their scope on “personal data”, however the definitions differ slightly. CCPA hereby understands all information that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household”, Sec. 1798.140(o)(1) CCPA. “Household” goes beyond the definition of the GDPR. It protects not only the consumer against misuse of his personal data, but also his family, for example, if conclusions can be drawn about the household when using personal data from other inhabitants of the same household. Sec. 1798.140(o)(1)(A)-(K) CCPA lists examples of indicators that contain commercial information regarding purchase history and consumption trends, Internet use or other electronic network activities such as browser history, interactions with apps, websites, geolocation data and interferences resulting from other personal data to create a consumer profile that describes preferences, behaviors and characteristics. In contrast to the GDPR, the CCPA stipulates in Section 1798.140(o)(2) that publicly accessible data held by government agencies are not covered by the scope of the CCPA. CCPA also does not provide increased protection for sensitive data categories, such as the political opinion or sexual orientation of the individual. Although CCPA stipulates “deidentified” data and GDPR “anonymized” data, their concepts in this respect are similar. Pseudonymization definitions in both laws are similar, both require technical controls to prevent reidentification.

The CCPA grants rights for data subjects, comparable to those of the European framework:

- Right to delete – Sec. 1798.105 CCPA

The CCPA grants the consumer a right to have its personal data deleted. The business can only refuse the data subjects' request for one of the reasons listed in Sec. 1798.105(d)(1)-(9) CCPA, for example if the use of the personal data is necessary for a contractual relationship. CCPA and GDPR have similar data erasure rights, nevertheless the GDPR requires one of six specific conditions for the request, whilst the CCPA right is broader for both sides, data subjects and data controllers.

- Right to information, disclosure and access – Sec. 1798.100(d), 1798.110, 1798.115 CCPA

A company may be requested by the consumer to inform about the processing of its personal data and to receive additional details regarding the personal data a business collects, as well as the purposes for processing the personal data. These provisions are comparable to Arts. 13, 14 GDPR. Nevertheless, CCPA limits these rights to a twelve-month period preceding the request. The CCPA offers only the right to obtain a written disclosure of the information in a portable format whilst the GDPR allows broader access not limited to such written disclosure.

- Right to opt-out of sale or sharing – Sec. 1798.120 CCPA

If a consumer chooses the opt-out option, the company must respect this and may only try to obtain consent again after twelve months, Sec. 1798.135(a)(5) CCPA. The GDPR requires consent of the consumer for the transfer (opt-in option). Section 1798.135(a)(1) CCPA stipulates that companies must display a clearly visible link on their website entitled "Do Not Sell My Personal Information" that prohibits the sale of personal data. The GDPR does not include a right to opt-out specifically from personal data sales, it contains however other rights a data subject may use to obtain a similar result in certain circumstances.

- Right of no retaliation – Sec. 1798.125 CCPA

The CCPA states that a "business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights". The GDPR implicitly grants that in Recital 39.¹¹⁰¹ Under the CCPA, businesses may also offer financial incentives if they inform the consumer and require opt-in consent. This "pay for privacy" approach is unknown to the GDPR, thus looks like a loophole and could lead to pressuring Californians to surrender their privacy rights, especially if the data subjects are economically inequal to others.¹¹⁰²

- Right to data portability – Sec. 1798.130 CCPA

The right to data portability ensures that the data subject receives the data that it has made available to a company in a portable and, as far as technically feasible, in an easy-to-use format to transmit these data to other companies without hindrance. The company must comply with this within 25 days and free of charge. Unlike the GDPR, which does

¹¹⁰¹ "Any processing of personal data should be lawful and fair."

¹¹⁰² The California Privacy Rights Act now expands this approach by allowing "financial incentives" for certain data processing and allows such actions also for "sharing", not just for "sale".

not explicitly regulate what time frame the right under Art. 20 GDPR covers, the CCPA applies this in Sec. 1798.130(a)(2) only for the past twelve months.

- Law of action – Sec. 1798.150(a)(1) CCPA

A private individual can only take legal action against a business if nonencrypted and nonredacted data has been illegally circulated and the business has not fulfilled its obligation to provide an adequate level of data security. In all other cases, only the Attorney General is authorized to bring the action. Violations in the form of an intentional breach of data protection obligations against the CCPA are subject to a penalty of USD 7.500,00; USD 2.500,00 in the case of a negligent breach. A penalty can only be avoided if the company meets the consumer's demands within 30 days. There are also normalized legal damages of USD 100,00 to USD 750,00 per inhabitant and incident, should companies become victims of data theft or other forms of data loss due to insufficient data security. Art. 79 GDPR, on the other hand, enables data subjects pursuant to take legal action against any violation of the law. Thus, CCPA and GDPR are substantially different when it comes to judicial redress.

On 3 November 2020, California citizens voted on the POTUS, Congressmen, and several popular petitions. 56 percent of voters voted for the California Privacy Rights Act (CPRA)¹¹⁰³, a law which was based on a citizens' initiative reflecting their interest in a functioning data protection system to control the handling of personal data.¹¹⁰⁴ The proposed initiative had originally been filed with the California Attorney General on 25 September 2019, but an amended ballot initiative was received by the Attorney General on 13 November 2019.¹¹⁰⁵ The CPRA becomes effective on 1 January 2023, with enforcement commencing on 1 July 2023. On 8 June 2022, Executive Director Ashkan Soltani was unanimously authorized to begin the CPRA rulemaking process to update "pre-existing California Consumer Privacy Act regulations to harmonize them with CPRA amendments and operationalizes and consolidates requirements within the law so it is easier to follow and understand. [...] The agency has previously said it will likely miss an initial July 1 statutory deadline to adopt regulations, but has not discussed whether that deadline, and thus enforcement, will be extended."¹¹⁰⁶ Since the CPRA would apply to legal entities that are located in California, the indirect scope extends beyond State borders. It would amend several provisions of the CCPA, resulting in – inter alia – these changes:

- Extends the B2B and "employee" exceptions through 31 December 2022;
- Extends the aforementioned 12-month "look-back" period for notice requirements;
- Adds the right of rectification and the right of restriction, both are similar¹¹⁰⁷ to those right in the GDPR;
- Extends the right to delete so that in the future businesses must also inform third Parties about the data subjects' request;

¹¹⁰³ California State. *California Privacy Rights Act of 2020 (CPRA), also known as Proposition 24*, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5, (3 November 2020).

¹¹⁰⁴ Ballotpedia. (3 November 2020). *California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*. [https://ballotpedia.org/California_Consumer_Personal_Information_Law_and_Agency_Initiative_\(2020\)](https://ballotpedia.org/California_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020)).

¹¹⁰⁵ California State. *Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment)*. https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf, (4 November 2019).

¹¹⁰⁶ Bryant, J. [Jennifer]. (9 June 2022). *CPPA board moves CPRA rulemaking process forward*. <https://iapp.org/news/a/cppa-board-launches-cpra-rulemaking-process>.

¹¹⁰⁷ Nevertheless, the right of restriction structured as an opt-out therefore does not go as far as the data subject right included in the GDPR.

- Extends information obligations;¹¹⁰⁸
- Requires that businesses obtain permission before collecting personal data from consumers younger than 16;
- Requires that businesses obtain permission from a parent or guardian before collecting personal data from consumers younger than 13;
- Adds the right against automated decision-making and requires that businesses disclose information regarding profiling algorithms used to determine a consumer's eligibility for financial or lending services, housing, insurance, and education admission, employment, or health care services;
- Requires that businesses collecting personal data for political purposes disclose the name of the candidates and committees for which the consumer's information was used;
- Adds risk assessment requirements relating to businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform an annual risk assessment and submit that assessment to the new "California Privacy Protection Agency" (CPPA)¹¹⁰⁹; California will thus be the first US State to have such an authority comparable to those in the EEA;
- Removes the ability of businesses to fix violations before being penalized for violations;
- Extends the right to opt-out so that in the future data subjects will be able to opt-out of any data sharing (even free of charge) for purposes of cross-contextual, behavioral advertising, while non-personalized advertising purposes will no longer be subject to opt-out requirements;
- Changes the "Do Not Sell My Personal Information" link to "Do Not Sell or Share My Personal Information", adds a second link "Limit the Use of My Sensitive Personal Information";
- Expands the definition of sensitive personal data;¹¹¹⁰
- Expands the private right of action and includes violations of more data categories in the event of an inadequate level of data security.

Virginia's "Consumer Data Protection Act" (VCDPA)¹¹¹¹ also took a comprehensive approach. It applies "to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data", Sec. 59.1-572. Although the VCDPA guarantees the majority of the consumers rights like GDPR and CPRA, it comes with a variety of exemptions. It does not include a natural person acting in a commercial or employment context. The Act also exempts 14 types of personal data, nonprofit

¹¹⁰⁸ The required notice would be expanded to several new terms, including the categories of "sensitive personal information" that are collected and "shared," and the length of time the business intends to retain each category. Consumers must now be informed about how long the company intends to keep the respective categories of personal data and sensitive personal data, or the criteria according to which this period is determined. It will be of practical importance for companies that the CPRA prohibits the companies from keeping such information longer than is reasonably necessary for the purpose of the processing.

¹¹⁰⁹ CPPA started its work on 1 July 2021. It is led by a five-person governing body with expertise in data protection, technology, and consumer rights. This body appoints an executive director. The agency has the task of implementing and enforcing laws protecting consumer privacy. Its broad, self-budgeted mandate includes issuing additional administrative regulations under the CPRA by the end of 2022, conducting audits and hearings, and conducting public awareness-raising efforts. Like other US authorities, it finances itself through the fines received.

¹¹¹⁰ The CPRA includes now a harms-based concept which goes even beyond the definition of Art. 9(1) GDPR. Inter alia, interestingly, the contents of a consumer's private communications are also considered "sensitive personal data" in the CPRA ("Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website application, or advertisement."). Nevertheless, the CPRA falls behind the GDPR in two ways: A trade union membership is not considered to be "sensitive", and the CPRA does not have strict opt-in consent rules.

¹¹¹¹ Virginia State. *Consumer Data Protection Act*, SB 1392, <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53>, (2 March 2021).

organizations, institutions of higher education, and cases subject to the GLBA and the “Health Insurance Portability and Accountability Act” (HIPAA)¹¹¹². In contrast to the GDPR, the VCDPA is based on opt-out consent, and it does not include a private right of action; only the Virginia Attorney General can enforce the Act. Moreover, it does not include a right of restriction like GDPR and CPRA. In April 2022, three amendment bills to the VCDPA changed the right to delete into a right to opt out of processing by data brokers and added political organizations to the definition of excluded nonprofits, which lowered the level of protection of this Act.¹¹¹³ Therefore, “at some point, if multiple states go the way of Virginia, you might not even get companies to honor California’s [rules]”¹¹¹⁴.

The “Colorado Privacy Act” (ColoPA)¹¹¹⁵ is the third comprehensive State law and is similar to the VCDPA. The main difference between CPRA, VCDPA, and ColoPA lies in the private right of action.¹¹¹⁶ This right is guaranteed by the CPRA (although limited to certain violations), while VCDPA and ColoPA do not include it at all. Other differences concern the “allowed cure periods (the amount of time in which a company has to correct a mistake), the size of businesses the law applies to, and whether tools such as “authorized agents” can be used for opt-out requests (such as the setting in a web browser that automatically opts the data subject out of data sales on a web page, or a service where another person makes opt-out requests on behalf of the data subject).¹¹¹⁷

Connecticut’s “Act Concerning Personal Data Privacy and Online Monitoring”¹¹¹⁸ (CTDPA) is the fourth and – at the time of submission of this thesis – latest comprehensive US State law in effect. It is similar to the ColoPA and the VCDPA. It gives consumers data subject rights (for example, the right to erasure) comparable to the GDPR with respect to their personal data. Enforcement of the law for violations of the law is the responsibility of the Attorney General. Like ColoPA and VCDPA, the CTDPA does not grant a private right of action for violations., though the CPRA does so (in a limited way).

¹¹¹² USA. *Health Insurance Portability and Accountability Act of 1996*, 104th US Congress, Public Law 104-191.

¹¹¹³ Adams, S. [Samuel]. (26 April 2022). *Virginia amendment process complete, text finalized, ahead of Jan. 1 effective date*. <https://iapp.org/news/a/vcdpa-amendment-process-complete-text-finalized-ahead-of-jan-1-effective-date>.

¹¹¹⁴ Feathers, T. [Todd]. (15 April 2021). *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*. <https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious>.

¹¹¹⁵ Colorado State. *Act concerning additional protection of data relating to personal privacy*, SB21-190, <https://leg.colorado.gov/bills/sb21-190>, (8 July 2021).

¹¹¹⁶ Desai, A. [Anokhy]. (7 July 2023). *US State Privacy Legislation Tracker*. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker>.

¹¹¹⁷ Klosowski, T. [Thorin]. (6 September 2021). *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*. *The New York Times*. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us>.

¹¹¹⁸ Connecticut State. *Act Concerning Personal Data Privacy and Online Monitoring*, S.B. No. 6, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022, (10 May 2022).

STATE	LEGISLATIVE PROCESS	STATUTE/BILL (HYPERLINKS)	COMMON NAME	CONSUMER RIGHTS							BUSINESS OBLIGATIONS				
				Right to access	Right to correct	Right to delete	Right to opt-out of certain processing	Right to portability	Right to opt-out of sales	Right to opt-in for sensitive data processing	Right against automated decision making	Private right of action	Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments
LAWS SIGNED (TO DATE)															
California		CCPA	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	X	X	X	X	X		L	16	X		X	
		Proposition 24	California Privacy Rights Act (2020; fully operative Jan. 1, 2023)	X	X	X	S	X	X	X	L	16	X	X	X
Colorado		SB 190	Colorado Privacy Act (2021; effective July 1, 2023)	X	X	X	P	X	X	X	X-	§13	X	X	X
Connecticut		SB 6	Connecticut Data Privacy Act (2022; effective July 1, 2023)	X	X	X	P	X	X	X	X-	§13	X	X	X
Indiana		SB 5	Indiana Consumer Data Protection Act (2023; effective Jan. 1, 2026)	X	X	X	P	X	X	X	X-	§13	X	X	X
Iowa		SF 262	Iowa Consumer Data Protection Act (2023; effective Jan. 1, 2025)	X		X		X	X		X-	§13	X		X
Montana		SB 384	Montana Consumer Data Privacy Act (2023, effective Oct. 1, 2024)	X	X	X	P	X	X	X	X-	§13	X	X	X
Tennessee		HB 1181	Tennessee Information Protection Act (2023; effective July 1, 2025)	X	X	X	P	X	X	X	X-	§13	X	X	X
Texas		HB 4	Texas Data Privacy and Security Act (2023; effective July 1, 2024)	X	X	X	P	X	X	X	X-	§13	X	X	X
Utah		SB 227	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	X		X	P	X	X			13	X		X
Virginia		SB 1392	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	X	X	X	P	X	X	X	X-	§13	X	X	X

Source: IAPP, “Comprehensive Consumer Privacy Bills”¹¹¹⁹

Currently, only four States in the US have comprehensive data protection laws being already effective: California, Virginia, Colorado, and Connecticut.

III. The role of the Federal Trade Commission

The FTC operates under the “Federal Trade Commission Act” (FTCA)¹¹²⁰, which empowers it to prevent “unfair or deceptive acts or practices in commerce”¹¹²¹. An act is unfair if “the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination”¹¹²². An act is “deceptive” if three elements are

¹¹¹⁹ IAPP. (7 July 2023). *Comprehensive Consumer Privacy Bills*.

https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf. // P = right to opt-out of processing for profiling/targeted advertising purposes; S = sensitive data; L = private right of action limited to certain violations only; ~ = right to opt out of certain automated decision making.

¹¹²⁰ USA. *Federal Trade Commission Act*, 15 U.S.C. §§ 41-58.

¹¹²¹ § 45(a)(1) FTCA.

¹¹²² § 45(n) FTCA.

met:¹¹²³ (1) There must be a representation, omission, or practice that is likely to mislead the consumer. (2) The act or practice must be considered from the perspective of the reasonable consumer. (3) The representation, omission or practice must be material. Moreover, the FTC “enforces a variety of other consumer protection statutes that prohibit specifically defined practices”¹¹²⁴. The FTC has great discretion in interpreting these terms. An unfair act exists, for example, if a data controller does not adhere to his contractually guaranteed data protection obligations.

If an inadmissible processing of personal data takes place in this context, the person concerned has no own rights.¹¹²⁵ Rather, it depends on the FTC to take the necessary measures through official orders or rulemaking. Its rulemaking authority stems from Sec. 18 FTCA, 15 U.S.C. § 57a, to formulate rules prohibiting unfair or deceptive acts or practices, which is, “a lengthy process that can take several years to complete. In July 2021, the FTC revised its Rules of Practice. It remains to be seen how these changes will impact the timeline”¹¹²⁶. Violations can be punished by civil penalties by bringing the case to suit in federal court against anyone who violates a trade regulation rule “with actual knowledge or knowledge fairly implied” that the act is unfair or deceptive and prohibited by the rule, 15 U.S.C. § 45(m)(1)(A). The FTC may also bring civil action against any person who violates a rule to redress injury to consumers or others, 15 U.S.C. § 57b(a)(1). Regarding the protection of children on the Internet, the FTC is also authorized to sanction the unauthorized processing of children’s data and to provide legal protection measures in favor of the parents and the child. The parents have claims to information, injunctive relief and surrender. Some of the data protection tasks are not performed by the FTC, but by the US Department of Commerce for data transfers from the EEA and Switzerland to the US. Since 21 July 2011, the newly created Consumer Financial Protection Bureau has been responsible for data protection in the financial area. Telecommunications providers also do not fall under the jurisdiction of the FTC, but the “Federal Communications Commission” (FCC).

In advance of the *Schrems II* judgment, some criticisms of the FTC had already been raised. First, the FTC’s authority is limited to its mandate under 15 U.S.C. § 45(a)(1), which “leaves aside any claims against government action”.¹¹²⁷ Moreover, the FTC “has no obligation to address the claim.”¹¹²⁸ As a result, it lacked “understandable and accessible guidance on how individuals can effectively enforce their rights”¹¹²⁹ and Privacy Shield offered “rather vague sanctions options under the dispute resolution bodies”¹¹³⁰. These bodies also had the problem of being “chosen and paid by the

¹¹²³ FTC. *FTC Policy Statement on Deception*,

https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf, (14 October 1983).

¹¹²⁴ FTC. (May 2021). *A Brief Overview of the Federal Trade Commission’s Investigative, Law Enforcement, and Rulemaking Authority*. <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>.

¹¹²⁵ “We can’t resolve your individual report, but we use reports to investigate and bring cases against fraud, scams, and bad business practices.” See FTC. (2023). *Report Fraud to the FTC*. <https://reportfraud.ftc.gov/#/>.

¹¹²⁶ IAPP. (December 2021). *FTC Privacy Rulemaking*.

https://iapp.org/media/pdf/resource_center/ftc_privacy_rulemaking_infographic.pdf.

¹¹²⁷ Boehm, F. [Franziska]. (August 2018). *Legal Expertise on the adequacy of the Privacy Shield*.

https://www.zar.kit.edu/DATA/veroeffentlichungen/237_Attachment_8_-_Expert_Review_by_Prof._Franziska_Boehm_a246a66.pdf. P. 25.

¹¹²⁸ Boehm, F. [Franziska]. (August 2018). *Legal Expertise on the adequacy of the Privacy Shield*.

https://www.zar.kit.edu/DATA/veroeffentlichungen/237_Attachment_8_-_Expert_Review_by_Prof._Franziska_Boehm_a246a66.pdf. P. 25.

¹¹²⁹ Boehm, F. [Franziska]. (August 2018). *Legal Expertise on the adequacy of the Privacy Shield*.

https://www.zar.kit.edu/DATA/veroeffentlichungen/237_Attachment_8_-_Expert_Review_by_Prof._Franziska_Boehm_a246a66.pdf. P. 27.

¹¹³⁰ Boehm, F. [Franziska]. (August 2018). *Legal Expertise on the adequacy of the Privacy Shield*.

https://www.zar.kit.edu/DATA/veroeffentlichungen/237_Attachment_8_-_Expert_Review_by_Prof._Franziska_Boehm_a246a66.pdf. P. 28.

companies and therefore not independent in the sense of EU data protection law”¹¹³¹. The CJEU made a similar point in *Schrems II*, stating that “data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data”¹¹³² and called for improvements to the US ombudsman mechanism because of its current failure to provide the requisite independent tribunal to ensure protections of Europeans’ rights.

¹¹³¹ Boehm, F. [Franziska]. (August 2018). *Legal Expertise on the adequacy of the Privacy Shield*. https://www.zar.kit.edu/DATA/veroeffentlichungen/237_Attachment_8_-_Expert_Review_by_Prof._Franziska_Boehm_a246a66.pdf. P. 29.

¹¹³² *Schrems II*. Para. 194

CHAPTER IV: ASIA-PACIFIC FRAMEWORK

Asia-Pacific (APAC) has grown in global economic weight in recent decades and is a region with a – by international standards setting – high momentum. The APAC market is growing the fastest among the world’s major regional markets with “six of the top 10 fastest-growing ecommerce economies in 2019 come from the Asia-Pacific region”¹¹³³. Member States of the “Association of Southeast Asian Nations” (ASEAN)¹¹³⁴ form a cooperation in Southeast Asia, which is the world’s fastest growing Internet region with nearly four million new users coming online every month over the next five years and E-Commerce related spending is expected to reach USD 200 billion by 2025.¹¹³⁵ “Digital technologies in ASEAN could be worth up to USD 625 billion by 2030. This is expected to contribute to the growth of its digital economy by 6.4 times, from USD 31 billion in 2015 to USD 197 billion by 2025.”¹¹³⁶

Regional cooperation between ASEAN and other APAC countries has been boosted by an agreement signed in mid-November 2020 by 15 countries from the Asia-Pacific region, the “Regional Comprehensive Economic Partnership (RCEP)”¹¹³⁷. What is questionable, however, is how variations in data protection laws of different countries are dealt with regionally. To this end, APAC’s two main frameworks – the “ASEAN Framework on Personal Data Protection”¹¹³⁸ and the “APEC Privacy Framework”¹¹³⁹ will be examined below.

China, as the strongest economy in this region and second largest economy in the world with a GDP of more than USD 18 trillion in 2023¹¹⁴⁰, recently strengthened the data protection rights of individuals with its “Personal Information Protection Law” (PIPL)¹¹⁴¹ and will therefore be explored more in detail as example for national regulation within APAC.

¹¹³³ APEC. *Regulations, Policies and Initiatives on E-Commerce and digital economy for APEC MSMEs' Participation in the Region*. https://www.apec.org/docs/default-source/publications/2020/3/regulations-policies-and-initiatives-on-e-commerce-and-digital-economy/220ecsgregulations-policies-and-initiatives-on-e-commerce-and-digital-economy-for-apec-msmes-particip.pdf?sfvrsn=63b748d7_1, (March 2020). P. 18.

¹¹³⁴ ASEAN Member States: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam.

¹¹³⁵ Thio, T.G. [Tse Gan]. (2018). *Data and privacy protection in ASEAN. – what does it mean for businesses in the region?*. <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf>. P. 4. // See also ASEAN. *ASEAN Data Management Framework*, https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf, (January 2021). P. 3.

¹¹³⁶ ASEAN. *ASEAN Data Management Framework*, https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf, (January 2021). P. 3.

¹¹³⁷ ASEAN. *Regional Comprehensive Economic Partnership Agreement*, <https://rcepsec.org/legal-text>, (1 January 2022). // RCEP includes Member States of ASEAN and its five FTA partners (Australia, China, Japan, New Zealand, and Republic of Korea).

¹¹³⁸ ASEAN. *Framework on personal data protection*, <https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf>, (November 2016).

¹¹³⁹ APEC. *APEC Privacy Framework 2005*, https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf, (2005).

¹¹⁴⁰ International Monetary Fund (IMF). (October 2022). *World Economic Outlook Database*. <https://www.imf.org/en/Publications/WEO/weo-database/2022/October>.

¹¹⁴¹ The National People’s Congress of the People’s Republic of China. *Personal Information Protection Law of the People’s Republic of China*, Chairman’s Order No. 91, (20 August 2021). // English translation used for this thesis can be found under <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021>.

I. Asia-Pacific Economic Cooperation (APEC)

APEC is an international forum for economic cooperation in the Pacific region, which was founded in Canberra in 1989 and initially met as an informal dialogue forum at ministerial level. Since 1993, the heads of the now 21 Member States have met annually as part of the APEC Economic Leaders Meeting to promote growth of Pacific Rim economies. Over the course of time, other key areas without direct economic policy relevance developed, such as the fight against international terrorism. Its Members include the US, China, Russia, Japan and Australia as well as other Pacific and South American countries.¹¹⁴² As an intergovernmental economic policy forum, objectives, measures, scope and success of the cooperation depend on the willingness of the Member States to what extent they are committed and work towards the goals. Decisions are only made by consensus and commitments are undertaken on a voluntary basis. Unlike the WTO or other multilateral bodies, APEC has no treaty obligations required of its Member States neither does it have any formal institutions beyond regular meetings and thus no institutionalized negotiation mechanism. The significance of the APEC economies cannot be doubted because they are “responsible for more than 60 percent of global economic output, account for 47 percent of world trade, and are home to 38 percent of the world’s population”¹¹⁴³.

1. APEC Privacy Framework 2005

APEC dealt with data protection for the first time in 2004 when it adopted the “APEC Privacy Framework”, which was further expanded in the following year. Herewith, it targeted the establishment of a system of data protection rules for companies. The goal was to “establish a more flexible framework within which member economies can develop their own laws and policies which are compatible with other economies in the region”¹¹⁴⁴. Its scope is territorial, subject to national law. Data controllers and (voluntarily) processors are included in the scope of application. The framework promoted a free flow of data and was of non-binding nature.

The framework included nine “APEC Privacy Principles” in part III: Preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and correction and accountability. Within the last principle, transborder data traffic was regulated based on the principle of accountability, which meant the controller being obliged to either obtain the data subject’s consent to transfer data abroad or to uphold the data protection standard of the country of origin also in the country abroad. The principle of accountability ensured that those affected by certain countries could rely on the fact that their domestic data protection standards were also being safeguarded when processing their personal data abroad.

These principles were related to those of the Privacy Shield. Both sets of rules contained limitation of purpose principles (“Uses of Personal Information” and “Data Integrity”) and the requirements of “Notice” and “Choice”. The principle of “Access and Correction” of the APEC Privacy Framework 2005 corresponded to that of the “Access” of the Privacy Shield, and “Accountability” to “Enforcement”. The Privacy Shield principle of “data integrity” largely corresponded to the requirements of the “Integrity of Personal Information” of the APEC Privacy Framework 2005 and the principle of “security

¹¹⁴² APEC. (2023). *Member Economies*. <https://www.apec.org/About-Us/About-APEC/Member-Economies.aspx>.

¹¹⁴³ Government of Canada. (2023). *Canada and the Asia-Pacific Economic Cooperation (APEC)*. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/apec/index.aspx?lang=eng.

¹¹⁴⁴ Kennedy, G. [Gabriela] and Doyle, S. [Sara] and Lui, B. [Brenda]. (2009). Data protection in the Asia-Pacific region. *Computer Law & Security Review*, 25(1), 59–68. P. 60.

safeguards” to the Privacy Shield provision of “security”. Only the rules on “Preventing Harm” and “Collection Limitation” of the APEC Privacy Framework 2005 were not found in this form in the Privacy Shield and the principles of “Accountability” and “Enforcement” differed in their specifications.

The principles of the APEC Privacy Framework 2005 fell behind those of the OECD Guidelines 1980 and the Directive 95/46 and were criticized “having a bias towards [the] free flow of information over privacy protection”¹¹⁴⁵. The APEC Privacy Framework 2005 was insofar weaker than the principles set out in the OECD Guidelines 1980 by not reproducing all the principles (they did not include Purpose Specification and Openness; see preamble and para. 5), lowering down the content of principles such as the “Purpose Specification Principle”, and at the same time improving some principles only in minor ways. The only new principles (“Preventing harm”, “Choice” and “Due diligence in transfers”) “carry inherent dangers and have little to recommend them”¹¹⁴⁶. Furthermore, it did not include considerations on how to treat the adequacy issue (Art. 25 Directive 95/46). Last, the APEC Privacy Framework 2005 ignored legislation and experience of privacy law in its region.¹¹⁴⁷ Thus, the APEC Privacy Framework 2005 was at least consistent with the OECD Guidelines 1980 and therefore only an acceptable framework on privacy principles forty years ago. Its principles were “for the most part unremarkable and deal with issues normally covered by international data protection laws”¹¹⁴⁸. Although it had a positive impact on economies in the Asian-pacific region without any data protection legislation by then, “it remained a policy document with little implication for cross-border regulation. [...] The limited regime is quickly being squeezed out as a viable regulatory model in the international political economy”¹¹⁴⁹. Accordingly, Marc Rotenberg, executive director of the EPIC, stated that the “APEC framework is backward looking. It is the weakest international framework for privacy protection, far below what the Europeans require or what is allowed for transatlantic transfers between Europe and the US, particularly because it focuses on the need to show harm to the consumer”¹¹⁵⁰. In addition, the rules for the implementation in national law were not strict enough since there were no detailed specifications and there was also no plan to monitor the implementation. There were also no requirements for TFPD (until the CBPR).

2. APEC Data Privacy Pathfinder and CPEA

In 2007, the “Data Privacy Pathfinder” was adopted to progress the implementation of the APEC Privacy Framework 2005.¹¹⁵¹ The majority of the Member States agreed to work together on conceptual implementation frameworks in the form of individual projects to increase consumer confidence in data protection and to strengthen the TFPD.

¹¹⁴⁵ Greenleaf, G. [Graham]. (2005). The APEC Privacy Framework - A new low standard. *Privacy Laws & Business International Reporter*, 11(5). <http://classic.austlii.edu.au/au/journals/PrivLawPRpr/2005/1.html>.

¹¹⁴⁶ Greenleaf, G. [Graham]. (2009). Five Years of the Apec Privacy Framework: Failure or Promise?. *Computer Law & Security Report*, 25(1), 28–43. P. 31. // Kennedy, G. [Gabriela] and Doyle, S. [Sara] and Lui, B. [Brenda]. (2009). Data protection in the Asia-Pacific region. *Computer Law & Security Review*, 25(1), 59–68. P. 61. // de Terwangne, C. [Cécile]. (2009). Is a Global Data Protection Regulatory Model Possible?. In S. [Serge] Gutwirth and Y. [Yves] Pouillet and P. [Paul] De Hert and C. [Cécile] de Terwangne and S. [Sjaak] Nouwt (eds.), *Reinventing Data Protection?* (pp. 175–189). Springer. P. 184.

¹¹⁴⁷ Greenleaf, G. [Graham]. (2009). Five Years of the Apec Privacy Framework: Failure or Promise?. *Computer Law & Security Report*, 25(1), 28–43. P. 32.

¹¹⁴⁸ Kennedy, G. [Gabriela] and Doyle, S. [Sara] and Lui, B. [Brenda]. (2009). Data protection in the Asia-Pacific region. *Computer Law & Security Review*, 25(1), 59–68. P. 61.

¹¹⁴⁹ Newman, A. L. [Abraham L.]. (2008). *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Cornell University Press. P. 103.

¹¹⁵⁰ CNET. (14 September 2007). *Google proposes global privacy standard*. http://news.cnet.com/Google-proposes-global-privacy-standard/2100-1030_3-6207927.html.

¹¹⁵¹ APEC. *APEC Data Privacy Pathfinder*, 2007/CSOM/019.

The “Cross Border Privacy Enforcement Arrangement” (CPEA)¹¹⁵² has been in place since July 2010. It is an outcome of the Data Privacy Pathfinder Initiative and “focuses on one of the four key goals of the APEC Privacy Framework, namely, to facilitate both domestic and international efforts to promote and enforce information privacy protections [and] aims to contribute to consumer confidence in electronic commerce involving cross-border data flows by establishing a framework for regional cooperation in the enforcement of Privacy Laws”¹¹⁵³. The “Privacy Enforcement Authorities” of the participating APEC Member States are public bodies that are responsible for the enforcement of data protection law and can initiate at least corresponding formal review procedures in the event of possible data protection violations. The Privacy Enforcement Authorities are facilitated by the CPEA to contact each other and to ask for administrative assistance within the framework of transborder review procedures; in suitable cases, the procedure can also be handed over entirely to another Privacy Enforcement Authority. However, any support remains at the discretion of the Privacy Enforcement Authority.

3. APEC Cross Border Privacy Rules

Based upon further work by the “APEC Electronic Commerce Steering Group” and the APEC Data Privacy Pathfinder of 2007, the “Cross Border Privacy Rules” (CBPR)¹¹⁵⁴ were elaborated and endorsed in November 2011. To date, economies participating in the CBPR system are Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, Chinese Taipei, and the United States.

Through the CBPR, “participating businesses and governments across the region are working together to ensure that when your personal information moves across borders, it is protected to the standards prescribed by the APEC Privacy Framework”¹¹⁵⁵. The aim is to increase data protection and to facilitate the free flow of data. The CBPR are a non-treaty framework. The CBPR system is like the Privacy Shield, as it provides means for self-assessment, compliance review, acceptance, and enforcement. A participating company can impose CBPR standards on itself, which consist then of group-internal policies on data protection to comply with established standards for the protection of personal data, which is like the system of BCR enshrined in Art. 47 GDPR.

“Participating companies are required to adhere to the standards established by the APEC CBPR system and to domestic laws in the economies in which they operate”.¹¹⁵⁶ Thus, the CBPR system does not replace domestic laws but functions independently of them. If there are no data protection standards in CBPR Member States, the CBPR system sets a minimum standard of data protection in those Member States. In those countries, however, where data protection requirements exist, they remain unchanged even if the Member State joins the CBPR system. If the Member States’ requirements go beyond those of the CBPR system, the further national regulations are decisive. This is a major difference to the GDPR, which is a directly applicable regulation.

A prerequisite for a company to participate in the CBPR system is that the State in which the company is established is a Member State of CBPR. A distinction must therefore be made between the participation of this country as such, and the participation of a

¹¹⁵² APEC. *APEC Cross-border Privacy Enforcement Arrangement (CPEA)*, <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement>, (September 2021).

¹¹⁵³ APEC. *APEC Cross-border Privacy Enforcement Arrangement (CPEA)*, <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement>, (September 2021).

¹¹⁵⁴ APEC. *Cross Border Privacy Rules System*, <http://cbprs.org/documents>, (November 2011).

¹¹⁵⁵ APEC. *Cross Border Privacy Rules System*, <http://cbprs.org/documents>, (November 2011).

¹¹⁵⁶ APEC. *Cross Border Privacy Rules System*, <http://cbprs.org/documents>, (November 2011).

company based in this country. A State's participation in the CBPR system requires a written application which must include that at least one national SA is participating in the CPEA. In addition, each CBPR Member State must define an independent so-called "Accountability Agent" (AA) responsible for evaluating and approving privacy policies and practices of companies. The AA also monitors and enforces companies' compliance with the CBPR provisions. In appropriate cases, they are also required to report non-compliance to those authorities assigned by the CPEA.

If a country is successfully included in the CBPR system, the companies based there can apply to participate, with such an application being made voluntarily. A company that requests to be included in the CBPR system must conduct a self-assessment and to respond to a questionnaire, the so-called "Intake Questionnaire" to demonstrate that their data protection rules meet the requirements of the APEC Privacy Framework. After a CBPR certification, the respective company will be found in a publicly accessible directory and serves to inform consumers and other interest groups. The directory contains information about the responsible contact persons in the company and about contact points of the certifying accountability agent and the responsible Privacy Enforcement Agency. The publication of the certified companies in this list also promotes the enforcement of the CBPR requirements. It enables data subjects to contact the responsible authorities with questions and complaints about data protection violations. Only companies certified by an AA may display a seal, trust mark, or otherwise claim to participate in the CBPR System.

The concrete form of enforcement of the CBPR is left to the participating States. Compliance with the CBPR system for a certified company should in any case be enforceable by the AA and the respective data protection authorities. The enforcement agencies are to cooperate within the CPEA in the enforcement of the CBPR. Regarding AA, this enforceability should be provided either by means of legal regulations or a private contract that is concluded with the company.

As soon as a company has acquired its membership, the data protection standards of the CBPR are binding. Such requirements include protections such as notice and consent, and a process for filing consumer complaints, but do not go as far as the GDPR; there is no right to erasure, for example.

Both the European BCR and the APEC CBPR concern international transfers of personal data. Both have common features such as the concept of the controller (accountable for how data are processed) and processor (processes data on behalf of the controller). However, there are also differences. BCR only allow the transfer of personal data to other companies within their own group of companies, but not to third Parties outside of this group, whilst CBPR provide for the transfer of personal data from a certified company to other companies - including those that do not belong to its group-internal network - in APEC Member States. In view of this, it becomes clear why it is difficult for controllers to achieve interoperability between BCR and CBPR. Globally operating companies that strive for compatibility of different types of data protection regulations beyond a regionally existing transborder interoperability therefore have no choice but to obtain both, which results in corresponding efforts and costs. APEC therefore started working with the European Council to determine a more efficient use and interoperability of the CBPR and BCR instruments.

As the CBPR compliance directory showcases, there are currently not many companies participating, compared to the data flow volume between the participating States.¹¹⁵⁷ This may result from the “chicken and egg” problem, as Heyder called it: “Businesses are waiting for more APEC countries to join the CBPR system before they seek CBPR certification, and APEC countries are waiting for more interest from the business community before joining.”¹¹⁵⁸ Another problem is that CBPR apply only to data controllers and not to processors. Data processing scenarios with the participation of several onward transfers by processors and sub-processors is therefore still a challenging point to solve. Moreover, CBPR have a great reliance on third-party AAs that serve as the key certification bodies. Nevertheless, the CBPR system reduces cost and time with a single, consistent set of privacy standards, it “facilitates legal compliance, it can help comply with data export restrictions, and it promotes consumer trust. [...] CBPR could facilitate access to and compliance with significant trading blocks in Asia”¹¹⁵⁹.

4. APEC Privacy Framework 2015

The APEC Privacy Framework 2015¹¹⁶⁰ “draws upon concepts introduced into the OECD Guidelines 2013 with due consideration for the different legal features and context of the APEC region”¹¹⁶¹. It applies “to persons or organizations in the public and private sectors who control the collection, holding, processing, use, transfer or disclosure of personal information” (para. 10 commentary) and to the same extent that the laws of each Member State apply. The definition of personal data and the scope, which includes only natural persons, are the same as regulated in the GDPR, paras. 9, 10. However, the APEC Privacy Framework 2015 applies only to data controllers (“personal information controller”), not data processors, para. 10.

The framework “is consistent with the core values of the OECD Guidelines 1980”, para. 5. As participation in the CBPR is voluntary, commitments are only then legally enforceable once a company is included in the CBPR system. As a formal certification through CBPR is possible, the framework takes, compared to the OECD Framework 2013, a step further. One advantage of the CBPR system is that the bureaucratic effort is significantly lower than that of the BCR. The decisive factor for the success of the CBPR system is how consistently the Member States treat the question of control and enforcement. The “APEC Electric Commerce Steering Group” found that “challenges presented by these technologies such as security or privacy issues could hamper or even derail the development of the digital economy”¹¹⁶² and saw an area of improvement for the APEC region by creating

a coherent and interoperable legislation environment in the region to bridge the digital divide as well as facilitate domestic laws and regulations on relating issues. [...] APEC economies should align domestic laws with international standards such as OECD

¹¹⁵⁷ Cross Border Privacy Rules System. (2023). *Cross Border Privacy Rules System Directory*. <http://cbprs.org/compliance-directory/cbpr-system>.

¹¹⁵⁸ Heyder, M. [Markus]. (4 September 2014). *The APEC Cross-Border Privacy Rules—Now That We’ve Built It, Will They Come?*. <https://iapp.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come>.

¹¹⁵⁹ Woo, J. [Jesse]. (30 October 2018). *As Asia-Pacific rises and integrates, so too could the APEC Cross-Border Privacy Rules*. <https://iapp.org/news/a/as-asia-pacific-rises-and-integrates-so-too-could-the-apec-cross-border-privacy-rules>.

¹¹⁶⁰ APEC. *APEC Privacy Framework 2015*, <https://www.apec.org/apecapi/publication/getfile?publicationId=42d9fa81-f683-46a8-858b-1cde61fdb8f8>, (August 2017).

¹¹⁶¹ APEC. *APEC Privacy Framework 2015*, <https://www.apec.org/apecapi/publication/getfile?publicationId=42d9fa81-f683-46a8-858b-1cde61fdb8f8>, (August 2017).

¹¹⁶² APEC. *Regulations, Policies and Initiatives on E-Commerce and digital economy for APEC MSMEs’ Participation in the Region*. https://www.apec.org/docs/default-source/publications/2020/3/regulations-policies-and-initiatives-on-e-commerce-and-digital-economy/220ecsgregulations-policies-and-initiatives-on-ecommerce-and-digital-economy-for-apec-msmes-particip.pdf?sfvrsn=63b748d7_1, (March 2020). P. 18.

guidelines and UN guidelines on Consumer Protection which serve as main international reference framework. As for economies still lacking the E-Commerce legislation to provide appropriate online legal protection, they should soon adopt those required legislative instruments to support ecommerce and enhance trust in online transactions among business and consumers.¹¹⁶³

II. Association of Southeast Asian Nations (ASEAN)

ASEAN is an international organization with political, economic and cultural objectives, with each member country developing its own regulation. Its regulatory frameworks are on a voluntary basis, such as those below mentioned on TFPD. In this “lies the difference between the EU and ASEAN - while the EU has a parliament with the power to legislate, ASEAN has the ASEAN Inter-Parliamentary Assembly with the power of persuasion.”¹¹⁶⁴

1. ASEAN Framework on Personal Data Protection

The “ASEAN Framework on Personal Data Protection” is a multilateral data protection agreement that aims to harmonize different regulations. In scope are theoretically both public and private sector, whereby a participating State can “exempt any areas, persons or sectors from the application of the Principles”, para. 4(a). Matters relating to “national sovereignty, national security, public safety, public policy and all government activities deemed suitable by a Participant to be exempted”, para. 4(b). This framework provides a guideline for a minimum level of protection, while allowing that “two or more Participants may enter into separate agreements to further strengthen collaboration on personal data protection in furtherance of the objectives of this Framework where practicable”, para. 5. Economies implementing this framework at a domestic level “may adopt exceptions that suit their particular domestic circumstances, and the framework does not create legally binding domestic or international obligations of any type”¹¹⁶⁵ The framework does not provide for an oversight body and enforcement measures are limited to mere consultation. Transborder data transfers are to be permitted either based on consent of the data subject or if “reasonable steps” are taken “to ensure that the receiving organization will protect the personal data consistently with these principles”.

2. ASEAN Framework on Digital Data Governance

The “ASEAN Framework on Digital Data Governance”¹¹⁶⁶ identifies four priorities and corresponding pillars with voluntary legal force: ASEAN Data Classification Framework, ASEAN Cross Border Data Flows (ASEAN CBDF) Mechanism, ASEAN Digital Innovation Forum, and ASEAN Data Protection and Privacy Forum.

On 22 January 2021, ASEAN Digital Ministers’ Meeting approved the “ASEAN Data Management Framework” (ASEAN DMF)¹¹⁶⁷ and the “Model Contractual Clauses for

¹¹⁶³ APEC. *Regulations, Policies and Initiatives on E-Commerce and digital economy for APEC MSMEs’ Participation in the Region*. https://www.apec.org/docs/default-source/publications/2020/3/regulations-policies-and-initiatives-on-e-commerce-and-digital-economy/220ecsgregulations-policies-and-initiatives-on-ecommerce-and-digital-economy-for-apec-msmes-particip.pdf?sfvrsn=63b748d7_1, (March 2020). P. 75.

¹¹⁶⁴ Thio, T.G. [Tse Gan]. (2018). *Data and privacy protection in ASEAN. – what does it mean for businesses in the region?*. <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf>. P. 6.

¹¹⁶⁵ GSMA. (September 2018). *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC can Protect Data and Drive Innovation*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf. P. 58.

¹¹⁶⁶ ASEAN. *ASEAN Framework on digital governance*. https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf.

¹¹⁶⁷ The “ASEAN Data Classification Framework” has been renamed as the “ASEAN Data Management Framework” // ASEAN. *ASEAN Data Management Framework*, https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf, (January 2021).

Cross Border Data Flows” (ASEAN MCC)¹¹⁶⁸. The ASEAN DMF emerged from the first pillar of the ASEAN Framework on Digital Data Governance and shall “promote sound data governance practices by helping organizations to discover the datasets they have, assign it with the appropriate categories, manage the data, protect it accordingly and all these while continuing to comply with relevant regulations.”¹¹⁶⁹. It is intended to provide organizations in Member States with an effective tool to achieve accountability and oriented towards a full data lifecycle from “governance and oversight” until “monitoring and continuous improvement”, which covers more than TFPD but also non-personal data scenarios. The ASEAN CBDF mechanism, which

relies on tested existing transfer mechanisms can help ensure that appropriate safeguards are in place, so that data privacy and security are protected when data are transferred across borders, while also ensuring that home country regulators retain authorized access to that data. In addition to increasing trust among consumers and regulators, such a mechanism can also help provide certainty for businesses around data transfers [...] and should seek [Member States] to restrict data transfers only in very limited circumstances (e.g., where companies have not adhered to their legal or regulatory requirements).¹¹⁷⁰

The ASEAN CBDF mechanism is proposed to be realized by adopting the dual-track approach, i.e., through a third party certification model and the use of the MCC. The latter emerged from the second pillar of the ASEAN Framework on Digital Data Governance. They are voluntary

contractual terms and conditions that may be included in the binding legal agreements between Parties transferring personal data to each other across borders [and Parties] may adapt these clauses with appropriate modifications at their discretion for transfers between businesses intra-country in AMS [ASEAN Member States], or transfers to non-AMS. Parties may, by written agreement, adopt or modify the MCCs in accordance with the principles set forth in the ASEAN Framework on Personal Data Protection (2016) or as required by any AMS Law. This does not preclude the Parties from adding clauses, by written agreement, as appropriate for their commercial or business arrangements so long as they do not contradict the MCCs. Parties are free to negotiate commercial terms provided they do not contradict the MCCs.¹¹⁷¹

The ASEAN MCC are a flexible template with optional supplemental obligations, as long as they are consistent with the ASEAN Framework on Personal Data Protection. The level of data protection set by the ASEAN MCC may not be undercut by national law, which prompted Hogan Lovells to issue this comment:

It is fair to say, however, that the Controller-Processor MCCs also include provisions representing “over-compliance”: i.e., obligations which are likely to exceed actual national law requirements and impose additional restrictions on transfers that are not found in the law. For example, in seeking to address the participation of ASEAN member states, which may not yet have regulations in place addressing cross border transfers, clause 2.1 sets a default that the data controller exporting the data to have

¹¹⁶⁸ ASEAN. *ASEAN Model Contractual Clauses*, https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf, (22 January 2021).

¹¹⁶⁹ ASEAN. *ASEAN Data Management Framework*, https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf, (January 2021). P. 4.

¹¹⁷⁰ US-ASEAN Business Council. (2023). *Digital Data Governance in ASEAN*. https://www.usasean.org/system/files/downloads/digital_data_governance_in_asean-key_elements_for_a_data-driven_economy.pdf. P. 17.

¹¹⁷¹ ASEAN. (22 January 2021). *ASEAN Model Contractual Clauses for Cross Border Data Flows*. http://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf. P. 4.

obtained data subject consent to the transfer, a requirement which proves onerous and outright prohibitive of cross border transfers in practice if the consent is revocable. [...] We expect, however, that organizations will continue to use bespoke forms of contract and legal terms that closer track mandatory local law requirements and avoid “over-compliance.”¹¹⁷²

There is no obligation to conclude ASEAN MCC in the case of TFPD but to choose other instruments: “self-assessment that transfer of data overseas shall be protected to a comparable level of protection, consent, codes of conduct, binding corporate rules, certifications, such as ISO [International Organization for Standardization] series relating to security and privacy techniques, APEC Cross Border Privacy Rules and Privacy Recognition for Processors Systems, or other legally enforceable mechanisms”¹¹⁷³. This “certification” mechanism as a ground for TFPD is still to be drafted. Unlike the Commission’s new SDPC, the ASEAN MCC contain only two modules: Controller-to-Processor and Controller-to-Controller. The biggest difference to the SDPC is that the ASEAN MCC are non-binding. They also have this deficiency compared to APEC’s CBPR, as the latter are of binding nature once the recipient is certified by the CBPR scheme.

III. Trans-Pacific Partnership and others

The “Comprehensive and Progressive Agreement for Trans-Pacific Partnership” (CPTPP)¹¹⁷⁴ was signed on 8 March 2018 with eleven countries being Parties¹¹⁷⁵ of the agreement. On 16 July 2023, Ministers responsible for trade from CPTPP Parties and the UK signed the UK’s Accession Protocol to enable the UK to join the CPTPP,¹¹⁷⁶ CPTPP would then include 23 countries with the UK.

CPTPP aims at comprehensive dismantling of tariffs between the contracting Parties within the framework of a free trade area. It contains provisions for the removal of further trade barriers and for the protection of intellectual property by private arbitration tribunals. If implemented in all signatory States, the CPTPP would be the third largest regional trade agreement after the EU and the “North American Free Trade Agreement” (NAFTA). The CPTPP provisions on E-Commerce prohibit discrimination in digital products, “data localization”¹¹⁷⁷, and require that Member States adopt online consumer protection provisions. Art. 14(8) CPTPP covers “personal information protection” and requires Parties to “adopt or maintain a legal framework” to protect personal information. Art. 14(10) CPTPP determines the principle of a free flow of data:

¹¹⁷² Hogan Lovells. (26 January 2022). *ASEAN Launches Model Contractual Clauses for Cross Border Data Transfers*. <https://www.jdsupra.com/legalnews/asean-launches-model-contractual-6923372>.

¹¹⁷³ ASEAN. (22 January 2021). *ASEAN Model Contractual Clauses for Cross Border Data Flows*. http://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf. P. 4.

¹¹⁷⁴ Australian Government, Department of Foreign Affairs and Trade. *CPTPP text and associated documents*, <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents>, (8 March 2018).

¹¹⁷⁵ Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore and Vietnam; on his first day in office, POTUS Trump had sealed the US withdrawal from the “Trans-Pacific Partnership” (TPP) and his successor Joe Biden has not yet reversed this. CPTPP was created in response to this withdrawal. CPTPP includes key TPP provisions but overrides 22 provisions that were supported only by the US but opposed by other countries. The TPP did not enter into force after the US withdrawal.

¹¹⁷⁶ Australian Government, Department of Foreign Affairs and Trade. (16 July 2023). *Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)*. <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership>.

¹¹⁷⁷ “Data localization” are forced requirements that confine data within a country’s borders by mandating companies to keep data within a certain border or by imposing additional requirements for data to be transferred abroad. Further below (Chapter VIII, Section I.) it is explained that “data localization” is only one type of a “data flow restriction”. We therefore prefer to use “data flow restriction” in the following. If “data localization” must be used in this thesis, it should generally be understood as a “data flow restriction” unless otherwise stated.

Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means. [...] Each party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

This Article also foresees measures deviant from this principle, but only

to achieve legitimate public policy objective[s], provided that the measure: is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and [when it] does not impose restrictions on transfers of information greater than are required to achieve the objective.

CPTPP has therefore a wide scope in relation to measures affecting trade by electronic means whilst excluding non-trade-related processing of personal data and such data held or processed by or on behalf of a government. The national laws of Member States can deviate from that principle only if they undergo a so-called “necessity test” before integrating exceptions. On local storage, Art. 14(13) CPTPP stipulates that “no party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory”. In CPTPP, measures inconsistent with this rule are only allowed if they include legitimate public policy objectives, and provided they are not “a disguised restriction on trade” or “impose restrictions on the use or location of computing facilities greater than are required to achieve the objective”.

RCEP encompasses countries which together account for about one-third of the world’s population and GDP. Even without India, which left the negotiations, RCEP is the largest trade area in the world. RCEP is an agreement exclusively on an economic level. Questions about human rights are almost not at all included. Compared to RCEP, the CPTPP aims for an even greater reduction in tariffs (up to 99 percent) as well as higher social and environmental standards and includes more restrictions for State-owned companies. There has been conflicting speculation during the negotiation process about whether transborder data flows and data flow restrictions would make it into the final RCEP text.¹¹⁷⁸ Arts. 12.4 and 12.5 RCEP now contain an obligation and security exception which says that

nothing in this Article shall prevent a Party from adopting or maintaining:

- (a) any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or
- (b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

The trilateral US - Mexico - Canada Free Trade Agreement (USMCA)¹¹⁷⁹, successor of NAFTA, was agreed to on 1 October 2018 and entered into force on 1 July 2020. Art. 19(11) USMCA stipulates that “no Party shall prohibit or restrict the cross-border transfer of information” and applies therefore similar rules as CPTPP. The USMCA includes possible exceptions if those have a legitimate purpose, are non-discriminatory, not a disguised restriction, and by means no greater than necessary, but only for data export

¹¹⁷⁸ EFF. (4 August 2017). *E-commerce RCEP Chapter: Have Big Tech’s Demands Fizzled?*. <https://www.eff.org/deeplinks/2017/08/e-commerce-rcep-chapter-have-big-techs-demands-fizzled>. // The RCEP draft contained a commitment to a free flow of transborder data and a ban on data localization (with exception clauses for each)

¹¹⁷⁹ USA. Office of the US Trade Representative. *Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text*, <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>, (1 July 2020).

limitations, which results in fact in a ban on data flow restrictions. The USMCA excludes – as the CPTPP – from scope “information held or processed by or on behalf of a Party [National Government], or measures relating to that information, including measures relating to its collection”, Art. 19(2) USMCA. Art. 19(8) USMCA provides that “each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)” and therefore sets the minimum standard for data protection according to these international agreements. Accordingly, Art. 19(8) USMCA sets also some principles: “limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.” The USMCA also includes the obligation for Member States to “endeavor to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction” and to inform about “how a natural person can pursue a remedy and an enterprise can comply with legal requirements”, Art. 19(8) USMCA. It also recognizes in Art. 19(8) USMCA the APEC CBPR as a “is a valid mechanism to facilitate cross-border information transfers while protecting personal information.”

IV. China

Data protection, data security and their regulation have played a role in China for some time, legislation in this area is nevertheless more recent (since 2017). It is becoming increasingly noticeable that China regulates data protection issues mainly for key technologies that require special framework conditions. This includes first and foremost cryptography and AI. China intends to achieve global supremacy for AI by 2030, both economically and politically. Kai-Fu Lee, author of the book “AI-Superpowers” highlighted in an interview some key facts about the rapid development in this sector. “China has three to four times more users than the US, fifty times more payment actions, ten times more food deliveries, three hundred times more shared bicycle rides, ten times more data than the US”, therefore, for China, “AI is fueled by data and data is the new oil”¹¹⁸⁰. However, China is not only focusing on AI. Starting in 2015, its strategical orientation¹¹⁸¹ recognized that “China’s manufacturing is still largely low-tech, low-skilled and based on cheap labor, and data is seen as crucial to innovation and economic upgrading. [...] China’s fast-growing e-commerce market is exceptionally strong, accounting for about 45 % of global transactions in that sector, and Chinese leaders want to capitalize on that strength.”¹¹⁸² Chinese regulations are associated with this to guarantee a safe development and use of new technologies. The regulatory intentions are also accelerated through trade with third countries, which have a higher level of data protection, and the fight against the misuse of personal data in China mainland.

¹¹⁸⁰ WGBH Educational Foundation, Frontline Documentary. (5 November 2019). *In the age of AI*. YouTube. <https://www.youtube.com/watch?v=tyGEEjOBdFc>.

¹¹⁸¹ In detail see Chapter IX, Section III.1.5.

¹¹⁸² Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 2.

1. Constitution

Arts. 38 and 40 of the “Constitution of the People’s Republic of China”¹¹⁸³ establishes rights that relate to privacy, such as a right of dignity of the person, prohibitions against insult, defamation, false accusation, or false information directed against Chinese citizens, and a right of freedom and secrecy of correspondence. These provisions do not, however, expressly establish a constitutional right to privacy.

2. Cybersecurity Law

The “Cybersecurity Law of the People’s Republic of China” (CSL)¹¹⁸⁴ has been in force since 1 June 2017. The CSL has a double focus. Despite its misleading title, the CSL not only refers to cyber security, but for the first time in Chinese regulation also contains rules on data protection and is therefore a subject of this thesis. This focus differs from EU legislation, where the two areas of regulation are separated from one another. The CSL leaves some terms vaguely defined. This has been corrected by the “National Standard of Information Security Technology - Personal Information Security Specification” (PI Specification 2018) and the revised 2020 version (PI Specification 2020)¹¹⁸⁵, both non-binding recommendations.¹¹⁸⁶ Art. 76(5) CSL defines “personal data” as “all kinds of information electronically or otherwise recorded that can independently or combined with other information be used to identify a natural person”. Anonymized data are not considered personal data, Art. 42 CSL. The scope of the CSL extends to natural persons who process personal data within the territory of the “People’s Republic of China” (PRC). The CSL applies to any natural person in the PRC whatever their nationality or place of residence. It applies to construction, operation, maintenance and use of networks, as well as the supervision and administration of cybersecurity within the territory of the PRC. It does not distinguish between data controllers and data processors but imposes obligations on “network operators” (which include both controllers and processors defined in the GDPR). The CSL does not exclude extraterritorial application. However, beyond an investigation below Art. 75 CSL, which can affect foreign companies with branches in China and foreign companies “that, for example, address Chinese customers with their website [and which can be] threatened with blocking their offers in China”¹¹⁸⁷, the CSL does not have an extraterritorial reach as the GDPR. The CSL regulates essential principles, also known from European data protection law (accountability, purpose limitation, consent, data minimization, openness, security) and data subject rights (access, erasure, rectification, portability) in the fourth Chapter of the CSL. Art. 41 CSL recognizes only consent as a legal basis to process personal data. Affected rights are provided in the form of a claim for data erasure and data correction. In addition, data security measures must be ensured, which are regulated in the third Chapter of the CSL. For network products of criticality, Art. 23 CSL specifies special requirements, e.g., IT security certification of products. The CSL primarily provides for administrative consequences if network operators violate their obligations. The competent authority can set a deadline for correcting illegal behavior and may impose a

¹¹⁸³ The National People’s Congress of the People’s Republic of China. *Constitution of the People’s Republic of China*, http://www.npc.gov.cn/zgrdw/englishnpc/Constitution/2007-11/15/content_1372964.htm.

¹¹⁸⁴ Creemers, R. [Rogier] and Triolo, P. [Paul] and Webster, G. [Graham]. (29 June 2018). Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017). *New America*. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china>.

¹¹⁸⁵ People’s Republic of China. *GB/T 35273-2020*, <https://web.archive.org/web/20201124083428/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>, (6 March 2020). // The definition of sensitive personal information, e.g., is further expounded upon in this PI Specification 2020.

¹¹⁸⁶ See further below in this Section.

¹¹⁸⁷ Kessler, F. [Florian] and Blöchl, J. [Jost]. (22 October 2018). *So wirkt Chinas Gesetz für Cybersecurity*. <https://www.divsi.de/so-wirkt-chinas-gesetz-fuer-cybersecurity/index.html>

fine if the illegal behavior is not corrected or leads to serious consequences. In addition, the competent authority can block websites, withdraw business licenses, confiscate illegal profits, freeze assets, and herewith also intervene directly on the business performance of the perpetrator. Fines can be imposed up to around EUR 150,000. The CSL provides rules for the transfer of personal data to third countries or international organizations. The main differences between those the GDPR and the CSL are the concept of adequacy and other multiple legal grounds for a TFPD, which the CSL does not recognize; the CSL mandates, in contrast to the GDPR, localization of personal data. The CSL does not establish that TFPD may be allowed where based on an adequacy decision, neither does it provide for other safeguards applicable to TFPD. Art. 37 CSL states that “operators of critical information infrastructure [OCII] that gather or produce personal information or important data¹¹⁸⁸ during operations within the mainland territory of the People’s Republic of China shall store such information/data within Mainland China”. Art. 23 CSL defines this “critical information infrastructure” as such which might seriously endanger national or public interests if damaged and tasked the relevant departments of the State Council with developing a catalogue of these infrastructures. Art. 2 of the “Critical Information Infrastructure Security Protection Regulations”¹¹⁸⁹ released in August 2021 define critical information infrastructure as “important network infrastructure, information systems, etc., in important industries and sectors such as public telecommunications and information services, energy, transportation, water, finance, public services, e-government, national defense science, technology, and industry, etc., as well as where their destruction, loss of functionality, or data leakage may gravely harm national security, the national economy and people’s livelihood, or the public interest.” From this general principle of data flow restriction, Art. 37 CSL includes an exception for those cases in which a data transfer is necessary for “business requirements”, if the security of the data transfer has been assessed according to the process specified by the “Cyberspace Administration of China” (CAC) or other relevant government agencies. The OCII concerned assume responsibility for the existence of this exception. Art. 66 CSL provides specific penalties for OCII that fail to comply with Art. 37 CSL. The following graphic highlights that enforcement in China has increased in recent years and similar levels are expected in the coming years. Since the publication of the DSL, the PIPL, and the “Measures for Data Export Security Assessment” (PRC Security Assessment Measures)¹¹⁹⁰, shares of “important data” can also be assigned.

¹¹⁸⁸ “important data” was left undefined in the CSL and the PI Specifications.

¹¹⁸⁹ Stanford University. (18 August 2021). *Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)*. <https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021>.

¹¹⁹⁰ People’s Republic of China. *Measures for Data Export Security Assessment*, http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm, (1 September 2022). (“PRC Security Assessment Measures”).



Source: Sinolytics GmbH, “Digital economy: Important data and personal information enforcement takes center stage in next three years”¹¹⁹¹

The CSL was supplemented and specified by the PI Specification 2018. The revised PI Specification 2020 was issued on 6 March 2020 and came into force on 1 October 2020. It contains “principles and security requirements for the collection, storage, use, sharing, transfer, public disclosure and deletion of personal data” and provides guidance as to best practice regarding the processing of personal data. This PI Specification 2020 applies not only to network operators to whom the CSL is applicable, but also to “processing activities carried out by all kinds of organizations. The document can also be used by competent authorities, third party assessment agencies and other organizations to supervise, manage and evaluate PI processing activities”. The PI Specification 2020 introduced modified requirements, the most important of which are addressed here:

- Personal information (Art. 3(1) PI Specification 2020):

Indicates that only natural persons are to be protected. “Network identification information” and “mobile phone number” have been removed from the definition.

- Processing (Art. 1 PI Specification 2020):

A “processing” is understood as “collection, preservation, use, sharing, transfer, disclosure, etc.” of personal data.

- Sensitive personal information (Arts. 3(2), 5(4), 6(3) PI Specification 2020):

Personal data are sensitive if “personal data that once disclosed, illegally provided or misused, may endanger personal and property safety, easily lead to personal reputation, physical or mental health damage or discriminatory treatment”. Additional requirements must then be satisfied prior to processing such data, data subjects must be separately

¹¹⁹¹ Sinolytics GmbH. (11 July 2022). *Digital economy: Important data and personal information enforcement takes center stage in next three years*. https://sinolytics.de/sinolytics_weekly.

informed of the purpose, method, scope and storage period of the processing of personal biometric information and biometric information be stored separately.

- Consent (Arts. 3(5), 5(6), 3(17), 5(3), 9(1a) PI Specification 2020):

A distinction is made between “consent” (general requirement for processing personal information, can also be implied from the data subjects’ conduct) and “explicit consent” (written or other positive action indicating consent required for specific processing scenarios, e.g., processing of sensitive personal data). No consent is needed if the processing is necessary for the execution or implementation of a contract as requested by the data subject. The concept of “business functions” is introduced and, accordingly, levels of consent required for “basic business functions” in contrast to “additional business functions” of a product or service. Whenever multiple business functions are offered, the controllers must avoid coercing users to agree to data processing by bundling services, they must obtain explicit consent, not repeatedly seek consent, not suspend or reduce the quality of other business functions if the data subject refuses to give consent for one business function, and not obtain consent surreptitiously by reason of improving service quality or user experience.

- Data subject rights (Art. 8(5) PI Specification 2020):

The right to cancel a data subject’s account with the network controller, together with additional requirements for network controllers to respond to those data subject’s requests.

- Risk assessment and personalized displays (Arts. 7(4), 7(5) PI Specification 2020):

The network operator must not infringe legitimate rights and interests of citizens, legal persons and other organizations, or carry out illegal actions. For a “personalized display”, content must be clearly marked as such, and users must be able to opt out. Requirement to conduct a data protection impact assessment before data aggregation and automatic decision-making mechanism.

- Data processing agreement and transfer to third Parties (Arts. 9(2), 9(6), 9(7) PI Specification 2020):

Whenever services are offered in cooperation with or via third-party providers, the service providers must check the ability of these third-party providers with regard to data security. The network operator needs to conclude a comprehensive data processing agreement with its processor or other third Parties to the respective processing, so that when a processor / partner does not comply with the agreement, the controller can require the processor / partner to stop the relevant processing, take remedial measures, mitigate security risks and terminate the agreement when necessary. Two controllers – if they are “common controllers” (the GDPR specifies these as “joint controllers”) – have to conclude an agreement to specify the security obligations and liabilities of each party. If the controller and the third party are not common controllers, the controller is required to establish a relevant “management mechanism” to control that the third party obtains consent from the data subject, to implement channels for data subjects’ complaints, conclude an agreement with such third party, disclose to the data subjects that the relevant product or service is provided by a third party, maintain relevant records, and require that the third party meets its legal obligations.

- Technical-organizational measures:

The network operator is required to consider the “Privacy by-Design” principle and to maintain and update “Records of Processing Activities” (RoPA). Additional requirements are introduced for the assignment of a DPO, who should have relevant work experience and expertise and whose responsibilities are further supplemented by the PI Specification 2020. If data processing is the main business, more than 200 employees are employed and over 500,000 individual data records are processed, a DPO must be appointed. The number of processed personal data records will be increased to 1 million people in the PI Specification 2020. This Specification also contains model clauses for data protection declarations that meet the requirements for clarity, correctness and completeness.

3. Civil Code

The “Civil Code of the People’s Republic of China” (Civil Code)¹¹⁹² became effective on 1 January 2021. Part I concerns “General Provisions” and Part V is concerned with “Personality Rights”. Part V “is not based on a precedent law that was incorporated into the Civil Code. Instead, regulations that were scattered in various laws were bundled together and supplemented by provisions in administrative regulations and court interpretations. The inclusion of personality rights in the Civil Code represents a significant development and innovation in Chinese law”¹¹⁹³. Within Part V, the law expressly provides – as one of the personality rights – the general right of privacy (Art. 110 Civil Code) and a general right to protection of personal data (Art. 111 Civil Code). Part V introduces a clearer legal basis for civil liability claims against infringements, including broader data breaches (Arts. 994 to 1000 Civil Code), definitions of privacy rights (Art. 1032 Civil Code) and of the protection of personal data (Art. 1034 Civil Code), actions that will or will not constitute an infringement of privacy rights (Art. 1033 Civil Code) or of the protection of personal information (Art. 1035 Civil Code). Data subject rights and obligations of data processors (also of data security nature) are regulated in Arts. 1037 to 1039 Civil Code and exceptions from liability arising from the violation of such obligations have ground in Art. 1036 Civil Code. Personal data may only be processed with the consent of the data subject or his/her guardian, except for anonymized data. Data subjects have the right to access and the right to correction.

4. Data Security Law

The “Data Security Law of the People’s Republic of China” (DSL)¹¹⁹⁴ entered into force on 1 September 2021. Its primary purpose is the protection of national security interests and other public interests. The DSL wants to set up a framework that classifies data collected and stored in China based on its potential impact¹¹⁹⁵ on China. The DSL is applicable to data processing activities carried out within the PRC. Nevertheless, “any organization or individual outside the territory of mainland China may also be held accountable to the law if such organization or individual harms the national security, public interests, or the lawful rights and interests of citizens or organizations of mainland China in carrying out data processing activities”¹¹⁹⁶. The DSL is an addition to the CSL

¹¹⁹² The National People’s Congress of the People’s Republic of China. *Civil Code of the People’s Republic of China*, <http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf>.

¹¹⁹³ Rödl & Partner. (5 August 2020). *China’s new Civil Code – Part 4: Personality Rights*, <https://www.roedl.com/insights/china-civil-code/part-4-personality-rights>.

¹¹⁹⁴ The National People’s Congress of the People’s Republic of China. *Data Security Law of the People’s Republic of China*, <http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>.

¹¹⁹⁵ “according to the data’s degree of importance in economic and social development, as well as the degree of danger to national security, public interests, or the lawful rights and interests of individuals or organizations brought about if it is altered, destroyed, leaked, or illegally obtained or used.”

¹¹⁹⁶ Clyde&Co. (28 October 2021). *Brief review of the Data Security Law*, <https://www.clydeco.com/en/insights/2021/10/brief-review-of-the-data-security-law>.

and adds to “network data” – as defined in the CSL – a new data type, which is “records of information by other means”, which is similar to “processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system” in Art. 2(1) GDPR. Art. 21 DSL distinguishes between “core data”¹¹⁹⁷, “important data,” and “ordinary data”. “Core data” includes “data related to [China’s] national security, lifeline of national economy, people’s livelihood and vital public interests” and is “presumably a subset of important data”¹¹⁹⁸. Same as in the CSL and the PI Specifications, “important data” was left undefined, and the government requested to publish a national-level catalog of such “important data”. “As a consequence, this enables the local government to flexibly adapt the protection of important data based on the varying requirements. At the same time, this also means that the local government has extensive freedom when it comes to classifying the data.”¹¹⁹⁹ “Ordinary data” are data “that have a minimal ability to impact society at large, or data that will only affect a small number of individuals or enterprises”¹²⁰⁰. Art. 25 DSL stipulates that “the State is to implement export controls in accordance with law for data belonging to controlled categories in order to safeguard national security and interests and fulfill international obligations”. This control, governed by Art. 22 DSL, is exercised by a “centralized and integrated, highly effective, and authoritative mechanism for data security risk assessment, reporting, information sharing, monitoring, and early warning”; this authority is the CAC, which is authorized to cooperate with the responsible department of the State Council to define suitable security management measures for transborder data transfer. According to Art. 31 DSL, data regarding critical information infrastructures, which is collected and obtained by companies in China, remains within the scope of Art. 37 CSL. This means that the DSL confirms the data localization principle introduced by the CSL. The DSL also echoed the CSL’s approach that a transborder data transfer is only lawful if a) the transfer is necessary for business requirements, b) a prior security assessment by the relevant authority has been conducted, c) a separate consent from individuals before transferring their personal data abroad has been obtained, d) an internal risk assessment¹²⁰¹ prior to the transfer has been conducted, and e) records of the assessment processing activities are kept. Art. 36 DSL states that organizations and individuals “must not allow to provide data stored within the mainland territory of the PRC to the justice or law enforcement institutions of foreign countries without the approval of the competent authorities of the PRC”; this means in this case that companies, even if they are not OCII, need the prior approval of the relevant authorities. Companies found in violation of those rules can face penalties of up to RMB 10 million, a forced shutdown of their businesses and potential criminal liabilities, depending on the type of data processed; this also includes “intermediary services”, which had obtained the data from their respective providers.

5. Personal Information Protection Law (PIPL)

PIPL, effective since 1 November 2021, applies to processing data of natural persons within the borders of the PRC, Art. 3 PIPL. PIPL herewith establishes the principle of territorial jurisdiction, supplemented by the rules of protective jurisdiction and can apply

¹¹⁹⁷ In other sources sometimes also translated as “critical data”, “core national data”, or “critical national data”.

¹¹⁹⁸ Luo, Y. [Yan] and Yu, Z. [Zhijing] and Liu, V. [Vicky]. (22 June 2021). *The future of data localization and cross-border transfer in China: a unified framework or a patchwork of requirements?*. <https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements>.

¹¹⁹⁹ Lelley, J.T. [Jan Tibor] and Yin, Y. [Yuanyuan]. (31 August 2021). *Cybersecurity & the New Data Security Law of the People’s Republic of China*. <https://buse.de/en/insights/cybersecurity-the-new-data-security-law-of-the-peoples-republic-of-china>.

¹²⁰⁰ Horwitz, J. [Josh]. (30 September 2021). China drafts new data measures, defines “core data”. *Reuters*. <https://www.reuters.com/world/china/issues-draft-rule-data-security-industry-telecoms-2021-09-30>.

¹²⁰¹ Like the TIA under the GDPR.

both “intraterritorial” and “extraterritorial”.¹²⁰² Processing activities by natural persons for “personal or family affairs” are exempted (Art. 72 PIPL). Unlike the CSL, which does not apply to the public sector, PIPL also applies to the processing of personal data “by people’s governments” (Art. 72 PIPL). “Personal data” is defined in terms of identifiability (Art. 4 PIPL). “Processing” has a broad definition in Art. 4 PIPL. “De-identification” is equivalent to “pseudonymization” in the GDPR and is considered personal data, whilst “anonymized” data are not (Arts. 4, 73 PIPL). Like CSL, PIPL recognizes the data type of “sensitive personal data”. PIPL recognizes also – albeit under a different wording – roles and responsibilities of “controller”¹²⁰³, “processor”¹²⁰⁴ and joint controllership (Arts. 20, 73 PIPL). Art. 6 PIPL includes the principles of purpose limitation and data minimization. Furthermore, a processing must be legitimate (Art. 5 PIPL), transparent (Art. 7 PIPL), accurate (Art. 8 PIPL), and secure (Art. 9 PIPL). Only under any of the seven conditions set out by Art. 13 PIPL, a controller may process personal data. Those conditions are alike those in the GDPR, with the exception of Art. 13(7) PIPL (“other circumstances provided for by laws and administrative regulations”), which is vaguer than the GDPR, as it does not specify what types of laws and administrative regulations can create such ground for data processing. If the data controller wants to rely on consent of the data subject (Art. 13(1) PIPL), this consent “shall be given by the individual concerned in a voluntary and explicit manner in the condition of full knowledge. If laws and administrative regulations provide that the processing of personal information shall be subject to the individual’s separate consent or written consent, such provisions shall prevail.”, Art. 14 PIPL. Herewith, the concept of “separate consent” is introduced, consent needs to be “unbundled”. Moreover, consent needs to be revocable and with sufficient notification. In the circumstances specified in Art. 13(1)-(7) PIPL, the data subject’s consent is not required. If the data processor intends to further process personal data for a purpose not related to the original one, it needs to inform data subjects and obtain consent. Data subjects can withdraw consent (Art. 15 PIPL). Data subjects shall be notified before processing (Art. 17 PIPL), except for confidential information and emergencies (Art. 18 PIPL). Personal data may only be stored for “the shortest time necessary to achieve the purposes of processing” unless regulations provide otherwise (Art. 19 PIPL), PIPL therefore also includes a principle of storage limitation. Data controllers¹²⁰⁵ have supervisory obligations over those they commission with processing activities (Art. 21 PIPL). A data controller which processes personal data for automated decision-making “shall ensure transparency in the decision-making and fairness and reasonableness in the processing results” and “options shall also be provided that do not target their specific personal characteristics” (Art. 24 PIPL). Surveillance “in public places shall be as necessary to preserve public safety, and shall comply with relevant national regulations, and have prominent alerts in place” (Art. 26 PIPL). A data controller has obligations – like those set by the GDPR – to comply with the PIPL (accountability principle), such as to establish mechanisms to process data subject request, take necessary security measures, designate a responsible DPO, undertake risk assessments, notify about data breaches, and maintain a RoPA, Arts. 49ff. PIPL. The CAC, relevant departments of the State Council, and also relevant departments of county-level and higher local governments are the enforcement authorities (Arts. 56ff. PIPL).

Art. 38 PIPL requires for lawful TFPD the satisfaction of one of the following measures:

¹²⁰² See Chapter VIII, Section III.

¹²⁰³ Equivalent in PIPL: “personal data processing entity”. This term could therefore be confusable with the “data processor” defined in the GDPR. This thesis will use the terminology of the GDPR.

¹²⁰⁴ Equivalent in PIPL: “third party”.

¹²⁰⁵ Again, in the sense of a data controller of the GDPR and this thesis’ terminology.

- passing a security assessment organized by the CAC unless exempted under Art. 40 PIPL from such an assessment by laws, regulations, or provisions of the CAC; or
- obtaining relevant certification from professional certification bodies as designated by the CAC; or
- conclusion of a contract with an overseas recipient according to the standard contract formulated by the state cyberspace administration, specifying the rights and obligations of both Parties; or
- where it has satisfied other conditions prescribed by laws, administrative regulations, or the State cyberspace administration.

The last three “transfer mechanisms” mentioned would only be an applicable transfer mechanism if no important data is transferred, the data controller is not an OCII, processes personal data of less than 1 million individuals, and the relevant TFPD does not involve personal data of more than 100,000 individuals and the cumulative transfer of personal data does not exceed 100,000 individuals or the transfer of sensitive personal data does not exceed 10,000 individuals (since January 1 of each preceding year).

In addition, each of these transfer mechanisms must meet these requirements:

- Data subjects have been informed about the details of the transfer and have given separate consent; and
- the necessary measures have been taken to ensure that the recipients of the extraterritorial data provide the same level of protection required under PIPL. In practice, this will involve prior due diligence, (amended) contractual clauses, and ongoing monitoring; and
- a “Personal Information Protection Impact Assessment” (PIPIA) has been conducted.

Art. 38 PIPL – same as Art. 13(7) PIPL – is significantly vaguer than the GDPR. Art. 38(5) PIPL stipulates that “where the international treaties and agreements that the People’s Republic of China has concluded or participated in have provisions on the conditions for providing personal information outside the territory of the People’s Republic of China, such provisions may be complied with”. It is yet unclear whether “such provisions may be complied with” is meant alternatively to Art. 38(1)-(4) PIPL or without prejudice to other grounds for transfers pursuant to Art. 38(1)-(4) PIPL. Interestingly, compared to the draft version of PIPL, one possible measure has been erased from the final version of PIPL, which is if the data export would have been necessary for international judicial assistance or administrative law enforcement assistance, in which case approval by the relevant regulatory authority would have been required, unless a treaty or agreement concluded by or participated in by China would have provided authority. Even with one or more of the aforementioned measures of Art. 38(1)-(5) PIPL being met, a data controller “shall take necessary measures to ensure that the processing of personal information by overseas recipients meets the personal information protection standards stipulated in this law”, Art. 38(6) PIPL. The interaction of Art. 38 PIPL and “other standards in this law” stipulated in PIPL (especially Art. 13 PIPL) is similar to the two-stages test within the GDPR, which was described above¹²⁰⁶. This means that the transfer must be necessary due to business requirements (Art. 38 PIPL), consent of data subjects must be obtained prior to the transfer and after provision of information¹²⁰⁷ to the data subject (Art. 39 PIPL), a “personal information protection impact assessment” must be conducted (Art. 55 PIPL), and a copy of this assessment retained (Art. 56 PIPL). It looks like – similar to the GDPR – that data subjects’ consent

¹²⁰⁶ Chapter II, Section II.3.4.4.a.

¹²⁰⁷ The identity and contact information of the data recipient(s), the purpose(s) and method(s) of data processing, the type(s) of personal information to be transferred; and how individuals can exercise their rights under the PIPL with respect to the data recipient(s).

must refer not only to the data processing activity as such (first stage) but also to the particular risk of a TFPD (second stage).

PIPL includes in Art. 40 PIPL – alike Art. 37 CSL – a general principle of data flow restriction, with similar exceptions.¹²⁰⁸ PIPL added additional requirements for two types of data controllers (which can also be non-OCII) distinguished based on the volume of personal data they process. Data controllers that process personal data reaching certain threshold amounts, as well as government authorities processing such data, are required to store such data within mainland China. There were no guidelines on how to classify and implement levels of protection according to types and amount of data, nor on which authorities Chinese law is referring to, which was burdensome to business operators.¹²⁰⁹ These threshold amounts are not defined in PIPL but, firstly, by the “Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data” of 11 April 2017, later by the “Measures for Security Assessment of Cross-border Transfer of Personal Information” of 13 June 2019, and lastly by the PRC Security Assessment Measures of 7 July 2022; the latter became effective on 1 September 2022 and replaced all previous measures.

PIPL distinguishes between a PIPIA of a responsible for a TFPD and a CAC-led assessment. The former is to be carried out for all cases of Art. 38(1)-(3) PIPL, while the latter is mandatory for the case of Art. 38(1) PIPL.

A data controller would be subject to a CAC-led assessment under some quantitative and qualitative circumstances.¹²¹⁰ These circumstances are refined in the PRC Security Assessment Measures, which supplements Art. 38(1) PIPL. It specifies the implementation of the requirements in line with the CSL, the DSL and the PIPL and therefore clarifies “the legal system for data cross-border transfer security assessment, with the Troika, say, the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law, acting as the upper-level laws and the [measures] and other refined legal documents forming the lower-level laws”¹²¹¹. The obligation to complete such CAC-assessment applies retrospectively to data transfers that have already been completed, with rectification to be completed no later than 1 March 2023. Criteria of this CAC-led assessment encompass

- the legality, legitimacy and necessity of the transfer and its scope; and
- the risks posed by the data security protection policies, laws and network security environment of the destination for the data, including whether the level of data protection regulation in the destination jurisdiction meets the corresponding standards under Chinese law; and
- the scale, scope, types and sensitivity of data to be transferred and the risk that the data may be tampered with, destroyed, leaked or lost; and

¹²⁰⁸ See in detail below Chapter VIII, Section I.

¹²⁰⁹ Lai, K. [Karry]. (11 November 2021). *Primer: China’s Data Security Law*. <https://www.iflr.com/article/b1vdlyc3c367qc/primer-chinas-data-security-law>.

¹²¹⁰ The PRC Security Assessment Measures specify that any of the circumstances below will require a CAC-led security assessment before any transborder data transfers out of China (outbound data) can occur: 1. Transfer of personal data and important data by OCII; or 2. Transfer of data includes important data; or 3. Transfer of personal data by a data processor who processes one million or more individuals’ personal data overseas; or 4. Cumulative transfer of personal data of 100,000 or more individuals or sensitive personal data (defined by PIPL) of 10,000 or more individuals; 5. Catch-all other circumstances to be specified by the CAC. // See Hogan Lovells. (12 July 2022). *China: updates on international data transfers*. <https://www.engage.hoganlovells.com/knowledgeservices/news/china-updates-on-international-data-transfers>.

¹²¹¹ Yangyang Su, P.C. [Peng Cai]. (12 November 2021). *China’s Data Cross-border Rules are about to Fall into Place. Comments on the Measures for Security Assessment of Data Cross-border Transfer (Exposure Draft)*.

[http://www.zhonglun.com/Content/2021/11-](http://www.zhonglun.com/Content/2021/11-12/1759271125.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration)

[12/1759271125.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration](http://www.zhonglun.com/Content/2021/11-12/1759271125.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration).

- whether data security and personal information rights and interests can be guaranteed; and
- whether the contract between the data exporter and importer fully specify the necessary responsibilities and obligations; and
- compliance with Chinese laws, regulations and agency rules; and
- other matters that the CAC considers necessary to assess.¹²¹²

These criteria are close to those of a TIA of the European framework,¹²¹³ besides (again) the vague expression “other matters that the CAC considers necessary to assess”, which gives the CAC (again) a broad discretion. Data exporters must submit an application letter, a PIPIA report, a copy of the data transfer agreement, and “other materials to be specified” (again, broad discretion by the CAC). The “Guidelines for Data Exit Security Assessment and Declaration (First Edition)” (“PRC Security Assessment Guidelines”) “cover how to apply for the CAC security assessment”¹²¹⁴ and

explain the procedures and processes for companies to apply for permission to export data out of China and include complete lists of required documents, templates for documents such as security assessment declarations, and application forms. The new guidelines follow the release of the finalized Measures for Data Export Security Assessment [PRC Security Assessment Measures].¹²¹⁵

The CAC would be required to decide if it will accept the application within 7 working days. After such acceptance, the CAC would have 45 working days to complete the assessment, with an extension to 60 working days in complex cases or where the CAC requires supplementary documents. Unsuccessful applicants can appeal to the State Cyberspace Administration for re-assessment no later than fifteen working days after receipt of an adverse assessment. The decision of the State Cyberspace Administration would then be final and be effective for 2 years, which guarantees a continuous supervision and possible re-assessments.

On 16 March 2023, the draft “Information security technology-Certification requirements for cross-border transmission of personal information”¹²¹⁶ (PRC Certification Specification) were released.¹²¹⁷ It supplements Art. 38(2) PIPL. This Certification mechanism may only be used – corresponding to PIPL’s extraterritorial reach – in scenarios of TFPD within the subsidiaries or affiliated companies of the same economic or business entity, or when overseas companies process personal data of natural persons within China from abroad for purposes such as providing products or services to natural persons in China, analyzing and evaluating the activities of natural persons in China, and other circumstances provided by laws and administrative regulations. The PRC Certification Specifications

¹²¹² Hogan Lovells. (12 July 2022). *China: updates on international data transfers*.

<https://www.engage.hoganlovells.com/knowledgeservices/news/china-updates-on-international-data-transfers>.

¹²¹³ See Chapter II, Section II.3.4.4.g.

¹²¹⁴ Huld, A. [Arense]. (6 June 2023). *Standard Contract Measures for Personal Information Export Come into Force June 1, Additional Guidelines Released*. <https://www.china-briefing.com/news/china-data-transfer-personal-information-export-standard-contract-procedures>.

¹²¹⁵ Huld, A. [Arense]. (5 October 2022). *China Releases First Guidelines for Cross-Border Data Transfer Application*. <https://www.china-briefing.com/news/china-releases-first-guidelines-for-cross-border-data-transfer-application>.

¹²¹⁶ People’s Republic of China. *Technical Specifications for Certification of Cross-Border Processing of Personal Information*, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381, (16 March 2023). (“PRC Certification Specification”).

¹²¹⁷ Those are almost identical to the Security Certification Specifications [People’s Republic of China. *Cybersecurity Standards Practical Guide – Security Certification Specifications for Cross-Border Processing of Personal Information V2.0*, (16 December 2022)], except for additional clarifications of certain definitions.

outline the basic principles and personal information (PI) protection standards for companies and overseas recipients of PI in the cross-border processing of PI, as well as the protection of the rights and interests of the PI subjects. [...] These requirements were formulated with the input of various government agencies, educational and research institutes, and technology companies, and serve as a legal basis for certification agencies. The Security Certification Specifications [PRC Certification Specification] also provide a basis for certification agencies to carry out certification of PI processors' cross-border processing activities and provide a reference for PI processors to regulate cross-border processing activities of PI.¹²¹⁸

Another transfer mechanism is to “conclude a contract with an overseas recipient according to the standard contract formulated by the state cyberspace administration”, Art. 38(3) PIPL. On 30 June 2022, the CAC published the “Standard Contract Measures for Personal Information Export” (PRC Standard Contract Draft), which supplements Art. 38(3) PIPL. The final version of the PRC Standard Contract was issued in March 2023 and became effective on 1 June 2023.¹²¹⁹ The PRC Standard Contract was accompanied by the “Guidelines for the Filing of Standard Contracts for Exporting Personal Information Abroad” (PRC Standard Contract Guidelines)¹²²⁰. In contrast to the new SDPC of the European framework,¹²²¹ the PRC Standard Contract contains only two modules covering the TFPD scenarios “controller-controller” and “controller-processor”; apart from that, they are similar to the SDPC.¹²²² A data controller is required to file an executed PRC Standard Contract with the provincial CAC within ten business days after the PRC Standard Contract becomes effective, together with a report on the PIPIA undertaken in respect to the TFPD.

For both legal bases set out in Art. 38 (2) and (3) PIPL, a prior PIPIA is necessary. The scope of such PIPIA is similar to the criteria of the CAC-led assessment mentioned above

and fulfils the requirement under Article 55 of the PIPL for data controllers to conduct a personal information protection impact assessment prior to the export of personal information. [This PIPIA] appears to resemble the adequacy assessments required under the European Union’s General Data Protection Regulation (GDPR), which may involve engaging local counsel in foreign jurisdictions to provide an opinion on how the laws in the destination jurisdictions will impact the foreign recipient’s performance of its contractual obligations.¹²²³

The PIPIA must cover:

- Whether the provision of personal information to overseas countries complies with laws and administrative regulations; and
- the impact on the rights and interests of individuals; and

¹²¹⁸ Huld, A. [Arense]. (28 March 2023). *China’s Draft Certification Standards for Cross-Border Personal Information Transfer (Updated)*. <https://www.china-briefing.com/news/draft-certification-standards-for-cross-border-processing-of-personal-information>.

¹²¹⁹ People’s Republic of China. *Standard Contract Measures for the Export of Personal Information*, http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm, (1 June 2023). (“PRC Standard Contract”).

¹²²⁰ People’s Republic of China. *Guidelines for the Filing of Standard Contracts for Exporting Personal Information Abroad (First Edition)*, http://www.cac.gov.cn/2023-05/30/c_1687090906222927.htm, (Mai 2023). (“PRC Standard Contract Guidelines”).

¹²²¹ See Chapter II, Section II.3.4.4.g.

¹²²² For a comparison of the PRC Standard Contract with the EU SDPC and the ASEAN MCC see below Chapter IX, Section III.1.4.1.

¹²²³ Kennedy, G. [Gabriela] and Woo, J. [Joshua]. (13 July 2022). *(Not So) Standard Contracts? Draft Standard Contracts Finally Released in China*. <https://www.mayerbrown.com/en/perspectives-events/publications/2022/07/not-so-standard-contracts-chinas-draft-standard-contractual-clauses-sccs-are-finally-released>.

- the impact of the legal environment and network security environment of overseas countries and regions on the rights and interests of individuals; and
- other matters necessary to safeguard the rights and interests of personal information.¹²²⁴

The overall effect is that PRC Security Assessment Measures and PRC Standard Contract “are graduated measures based on the nature of the [data controller] making the transfer and the volume of the personal information involved, whereas third party certification is only available in respect of two specific types of transfers – intra-group transfers and offshore collection/processing.”¹²²⁵ In comparison to other transfer mechanisms, the PRC Standard Contract is a “simpler procedure than the other options as it does not require an external audit”¹²²⁶.

The “Technical Specifications for Certification of Cross-Border Processing of Personal Information”¹²²⁷ (“PRC Technical Specifications”) “provide guidance for multinationals and other entities with a presence in multiple countries to comply with China’s requirements for cross-border personal information processing”¹²²⁸ and

some more clarity on some aspects of the law’s requirements, in particular for how large multinationals and entities with locations in both China and overseas can legally share personal information across borders. They also act as a guide for companies and certification agencies that assist companies in transferring the personal information of Chinese citizens overseas, putting forward the basic principles for processing and protection of personal information, requirements for all relevant parties in cross-border processing activities, and protection of the rights and interests of personal information subjects. Finally, they provide companies with a reference guide for regulating cross-border processing activities of personal information.¹²²⁹

Violations of the obligations under Art. 38 (1)-(3) PIPL may be sanctioned in accordance with the CSL, the DSL, the PIPL, or under criminal law provisions. However, a final answer to the question of what counts as “important data” is not possible even on the basis of these three legal bases to a TFPD, because only a general definition is included.¹²³⁰ With the exception of the automotive industry, legal uncertainty for organizations therefore remains about which of their personal data processed qualify as “important”.¹²³¹

¹²²⁴ Yang, S. [Samuel] and Fung, C. [Christopher] and Wu, L. [Leann]. (16 August 2022). *Will China’s new certification rules be a popular legal path for outbound data transfers?*. <https://iapp.org/news/a/will-chinas-new-certification-rules-be-a-popular-legal-path-for-outbound-data-transfers>.

¹²²⁵ Hogan Lovells. (12 July 2022). *China: updates on international data transfers*. <https://www.engage.hoganlovells.com/knowledgeservices/news/china-updates-on-international-data-transfers>.

¹²²⁶ Huld, A. [Arense]. (6 June 2023). *Standard Contract Measures for Personal Information Export Come into Force June 1, Additional Guidelines Released*. <https://www.china-briefing.com/news/china-data-transfer-personal-information-export-standard-contract-procedures>.

¹²²⁷ People’s Republic of China. *Technical Specifications for Certification of Cross-Border Processing of Personal Information*, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381, (16 March 2023). (“PRC Technical Specifications”).

¹²²⁸ Huld, A. [Arense]. (6 June 2023). *Standard Contract Measures for Personal Information Export Come into Force June 1, Additional Guidelines Released*. <https://www.china-briefing.com/news/china-data-transfer-personal-information-export-standard-contract-procedures>.

¹²²⁹ Huld, A. [Arense]. (11 May 2022). *New Specifications for Cross-Border Processing of Personal Information for MNCs*. <https://www.china-briefing.com/news/china-cross-border-personal-information-transfer-new-clarifications-for-multinational-companies/>.

¹²³⁰ Rödl & Partner. (10 August 2022). *Outbound Data Transfer Security Assessment Measures*. <https://www.roedl.com/insights/cross-border-data-transfer-china-security-assessment-measures>.

¹²³¹ Rödl & Partner. (10 August 2022). *Outbound Data Transfer Security Assessment Measures*. <https://www.roedl.com/insights/cross-border-data-transfer-china-security-assessment-measures>.

The legal bases of Art. 38 (1)-(3) PIPL are the final piece in the puzzle of China's way to an advanced and comprehensive data protection framework archetype.¹²³² Ning, Han, Minlv, and Honglv argued that “the mutually supporting and complementary provisions in the CSL, the DSL and the PIPL [therefore] form a comprehensive and complete superior legislation basis for the Measures [PRC Security Assessment Measures] to require “Data Processors” [meaning data controllers in the sense of the GDPR] to fulfill their security assessment obligations of cross-border data transfer.”¹²³³

¹²³² See in detail Chapter IX, Section III.1.

¹²³³ Ning, S. [Susan] and Han, W. [Wu] and Minlv, Y. [Yao] and Honglv, C. [Chen]. (17 December 2021). *Interpretation of the Measures on Security Assessment of Cross-border Data Transfer (Draft for Comment)*. <https://www.chinalawinsight.com/2021/12/articles/compliance/interpretation-of-the-measures-on-security-assessment-of-cross-border-data-transfer-draft-for-comment>.

CHAPTER V: INTERNATIONAL ORGANIZATIONS FRAMEWORK

The differences between the regulations described above for the three most important frameworks for TFPD also exist because different stakeholders are located in different countries. If a reconciliation of interests is not or cannot be done autonomously, there is a need for international law. The ICDPPC has therefore repeatedly called for global data protection rules. First articulated in the so-called “Montreux Declaration”¹²³⁴, this appeal was repeated by Commissioners in 2008 and 2009 through the draft of a global legal instrument on data protection with a view to submitting it to the UN. At the ICDPPC in Brussels in 2018, the Committee recalled that the so-called “Warsaw Declaration”¹²³⁵ “mandated an extension to the work of the International Enforcement Coordination Working Group to develop a common approach to cross border case handling and enforcement coordination, to be expressed in a multilateral framework document addressing the sharing of enforcement-related information, including how such information is to be treated by recipients thereof”.¹²³⁶

Since then, more regulations were created at international level, which are not clearly attributed to obligations or effects in international law, and which cannot be unequivocally classified in the traditional system of international law sources. These are mainly those adopted by international organizations which, according to their statutes, are non-binding, but nevertheless formulate rules that are relevant for the Parties. These include bi-, pluri- or multilateral treaties between States whenever they cannot be classified as international conventions due to the lack of a Party’s willingness to commit to enforceable legal obligations arising from the rules set out in those treaties. Those regulatory instruments are commonly referred to as “international soft law”.

Those instruments were not able to provide the required standards in the short term since this generation of law by means of international custom and international conventions was rather lengthy and cumbersome and involved many stakeholders. They were therefore not able to keep up with the rapidly changing conditions in areas of digitization, including data protection. This is also reflected by the relationship between the US and the EU in terms of the level of protection in data protection, which is still being attempted to be balanced out by means of increasingly overlapping bilateral agreements. International soft law does not have the quality of positive law. There is no direct binding effect and democratic legitimation. A violation of rules of international soft law generally does not result in an immediate sanction. Due to the lack of positive legal quality, there is the option of flexible reformulation in soft law rules. The rules international soft law, which are initially recognized and followed as informal practices in international legal relations, can, in the course of time, evolve towards normative structures. That way, the quality of international soft law can approach positive law both at the level of international custom and in the national legal systems. Ultimately, a process of this solidification takes

¹²³⁴ ICDPPC. *Montreux Declaration*, https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf, (2005). (“Montreux Declaration”).

¹²³⁵ ICDPPC. *Warsaw Declaration*, <https://icdppc.org/wp-content/uploads/2015/02/Warsaw-declaration-on-Applification-of-society-EN.pdf>, (2013). (“Warsaw Declaration”).

¹²³⁶ ICDPPC. *Resolution on exploring future options for International Enforcement Cooperation*, <https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-exploring-future-options-for-International-Enforcement-Cooperation-2017.pdf>, (2017).

place through repeated application and growing conviction of the correctness or appropriateness of underlying normativity. The debate on the subsumption of international soft law therefore became a point of irreconcilable disagreement and has produced a wide variety of views. For reasons of scope, this thesis cannot aim to analyze this dispute in detail. Rather, it should be assumed that international soft law as such can at least have certain legal effects, if not being a special form outside the recognized sources of international law (Art. 38 Statute of the ICJ¹²³⁷). International soft law might be considered as source within the catalogue of international law, if soft law instruments meet certain requirements of a formal source of international law beyond the types of legal production enumerated in Art. 38(1) Statute of the ICJ. In this respect, soft law could be a measure of not only a purely political or extra-legal phenomenon, but rather be seen as a partially binding legal instrument, which could serve as a measure for regulating TFPD.¹²³⁸

I. OECD

The OECD had a significant influence on the evolution of international data protection law. The origins of the OECD trace back to the 1960s, when 18 European countries as well as the US and Canada joined forces to promote economic integration and development as part of a common institution. In several rounds of expansion, the number of members has now grown to 38 States, spread across North and South America as well as Europe and Asia. These Member States work towards the creation of better policies for better lives. In addition to the Member States and partners, the Commission also takes part in discussions within the OECD. Although the status of the Commission goes far beyond that of an observer, it has no voting rights and does not officially participate in the adoption of legislation across the OECD Council.

1. Guidelines 1980

According to the economic orientation of the OECD, the motivation for the elaboration of the OECD Guidelines 1980 was to avoid national data protection levels becoming a barrier for international trade.¹²³⁹ At the same time they wanted to prevent companies from circumventing national data protection regulations by moving their data processing to a so-called “data haven” territory, a State with lower or no level of data protection. The OECD Guidelines 1980 assumed that a free TFPD in connection with clear data protection standards is economically desirable, while they are intended to help harmonize national regulations.¹²⁴⁰

All OECD members, except Turkey and the US – for its private sector –, have implemented the OECD Guidelines 1980. The OECD Guidelines 1980 related to both public and non-public areas, contained procedural and substantive regulations and were non-binding under international law. The scope of application of the OECD Guidelines 1980 was limited to natural persons, Art. 2(b) OECD Guidelines 1980, the inclusion of legal persons left to the Member States. It was also left to Member States to limit the OECD Guidelines 1980 only to automated data processing. In contrast to Convention 108, the OECD Guidelines 1980 only served as recommendations for national data

¹²³⁷ The Statute of the ICJ is an integral part of the UN Charter, as specified by Chapter XIV of the UN Charter, which established the ICJ. // ICJ. *Statute of the International Court of Justice*, <https://www.icj-cij.org/en/statute>, (1945).

¹²³⁸ See also Chapter XII, Section I.

¹²³⁹ OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, <https://www.uio.no/studier/emner/jus/jus/JUTPRIV/h05/undervisningsmateriale/oecd-pv.doc>, (23 September 1980). Preface.

¹²⁴⁰ OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, <https://www.uio.no/studier/emner/jus/jus/JUTPRIV/h05/undervisningsmateriale/oecd-pv.doc>, (23 September 1980). Preface.

protection regulations and were intended to provide governments with a framework for elaborating their own national data protection regulations. Although not legally binding, the OECD Guidelines 1980 have been “highly influential on the enactment and content of data protection legislation in countries outside Europe” and for the APEC Privacy Framework¹²⁴¹.

The OECD Guidelines 1980 appealed to the Member States to enable a free TFPD. They mainly dealt with the transfer of personal data to another Member State and, in this respect, were based on the equivalence of the level of protection in the recipient State. If the recipient country complied with the OECD Guidelines 1980, a data transfer should in principle not be restricted. Interestingly, the OECD Guidelines 1980 did not regulate a scenario if the data protection provisions of the issuing State are in danger of being circumvented by transferring data through another Member State to a non-Member State.

At the heart of the OECD Guidelines 1980 were eight privacy principles: Collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability. There were rules on the rights of data subjects and to promote self-regulation by companies.

The principles of the OECD Guidelines 1980 and of the Convention 108 were similar because of the co-operation between the two drafting bodies. Both did neither recommend nor require that a Member State establishes a SA. Neither did they deal directly with the conflict of laws.

However, the provisions on implementation and international co-operation were more developed in the Convention 108.¹²⁴² The OECD Guidelines 1980 did, compared to Convention 108, not contain specific requirements on the erasure or anonymization of personal data after a certain period; neither did they mention the need for special safeguards for sensitive personal data.¹²⁴³

In some points the OECD Guidelines 1980 were broader than Convention 108 by covering manual data processing, comprehensively formulating the “Openness Principle” (Art. 12 OECD Guidelines 1980), including a more general application of data flows between Member States (Art. 18 OECD Guidelines 1980), and urging the Member States to “encourage and support self-regulation, whether in the form of codes of conduct or otherwise” (Art. 19(b) OECD Guidelines 1980).¹²⁴⁴

The Guidelines were only “minimum standards [...] capable of being supplemented by additional measures for the protection of privacy and individual liberties”, Art. 6 OECD Guidelines 1980. The little concrete formulations, the wide leeway for implementation and the broad exemptions from data protection principles made the OECD Guidelines 1980 a “dull sword”. Its effect lied more in the political arena, as they concerned the first international minimum consensus on data protection.

¹²⁴¹ Bygrave, L. A. [Lee A.]. (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar. P. 28.

¹²⁴² Bygrave, L. A. [Lee A.]. (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar. P. 27.

¹²⁴³ Bygrave, L. A. [Lee A.]. (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar. P. 27.

¹²⁴⁴ Bygrave, L. A. [Lee A.]. (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar. P. 27–28.

2. Guidelines 2013

With the OECD Guidelines 2013, existing provisions have been partially modernized and some new data protection concepts have been included. However, the general principles remained unchanged, which was seen as a missed opportunity to react to technical novelties.¹²⁴⁵

Two new ideas dominated the changes to the OECD Guidelines 2013. Firstly, a focus on the implementation of data protection through a risk management approach. A new part three – “Implementing Accountability” – recommends the implementation of a data protection management program, including that data controllers must be prepared to demonstrate that the program is up and running and that data security breach notifications are observed. This strengthened the Guidelines’ “accountability” and “security” principles. Secondly, the need to address the global dimension of data protection through improved interoperability. The OECD Council therefore “invites non-Members to adhere to this recommendation and to collaborate with Member countries in its implementation across borders”¹²⁴⁶. It is questionable whether this shall mean that any references to a “Member country” in the Guidelines should be understood as a reference to “an adhering country” – whether or not a Member – and if a non-Member can now adhere to the Guidelines by “simple declaration”.¹²⁴⁷

The inclusion of “another country” in Art. 17 OECD Guidelines 2013 is a major change, because the OECD Guidelines 1980 only imposed restrictions on TFPD between “Member countries”. This could mean that whenever a country has “adhered” (as a Member or non-Member) to the OECD Guidelines 2013, Art. 17 OECD Guidelines 2013 could apply to any country adhering to the Guidelines and the country could then impose limitations on data exports to other countries in the world. A half sentence has been added to Art. 6 OECD Guidelines 2013: “...which may impact transborder flows of personal data.” In the view of the Supplementary Explanatory Memorandum, the OECD hereby could intend to confirm that additional measures under Art. 6 OECD Guidelines 2013 can also result in additional restrictions on TFPD set out in Art. 17 Guidelines 2013. This interpretation means that any country adhering to the OECD Guidelines 2013 shall allow data exports to any other country adhering to the Guidelines.

Although the OECD Guidelines 2013, same as the OECD Guidelines 1980, recommend that Member countries “should adopt laws protecting privacy” (Art. 19(b) OECD Guidelines 2013), the new Guidelines lack a restrict interpretation of how to implement.¹²⁴⁸ Moreover, the OECD Guidelines 2013 include a list of non-legislative measures. This could be seen as a shift of the OECD Privacy Framework towards approaches such as APEC’s CBPR or the US framework. Lastly, OECD Guidelines 2013 removed completely its former Art. 16, which stated that “Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure”. These

¹²⁴⁵ Greenleaf, G. [Graham] and Clarke, R. [Roger] and Waters, N. [Nigel]. (27 September 2013). International Data Privacy Standards: A Global Approach (Australian Privacy Foundation Policy Statement), *UNSW Law Research Paper* No. 2013-62, <http://dx.doi.org/10.2139/ssrn.2327325>. P. 2–3.

¹²⁴⁶ OECD Privacy Framework. P. 12.

¹²⁴⁷ Greenleaf affirms this interpretation. He adds that this would be “beneficial insofar as it functions to encourage countries without data privacy laws to adopt such laws to a consistent minimum standard”. See Greenleaf, G. [Graham]. (2017). *Asian Data Privacy Laws*. Oxford University Press. P. 540.

¹²⁴⁸ Guidelines 1980: “that Member countries take into account their domestic legislation” and “endeavor to adopt appropriate domestic legislation” // Guidelines 2013: “implement the Guidelines through processes that include all relevant stakeholders”.

“weakened cross-border data transfer provisions”¹²⁴⁹ are a major deficiency of the OECD Guidelines 2013. Greenleaf/Clarke/Waters therefore resumed that “[the negative changes to OECD Guidelines 2013] are harmful in restricting the ability of countries to limit exports of personal information to jurisdictions with weaker privacy standards”.¹²⁵⁰

3. Global Privacy Enforcement Network

The “Global Privacy Enforcement Network” (GPEN)¹²⁵¹ is a network that serves the transborder enforcement of data protection regulations. The GPEN was launched by the OECD in 2010 and is based on a OECD recommendation in 2007 on transborder cooperation to enforce data protection law which provided that “Member countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns” and that data protection enforcement authorities “should co-operate with each other, consistent with the provisions of this Recommendation and national law, to address cross-border aspects arising out of the enforcement of Laws Protecting Privacy”.¹²⁵² Regulators from 50 countries are now involved in this network, including data protection regulators from most EU Member States.¹²⁵³ GPEN’s aim is similar to the CPEA in the APAC framework. GPEN can in principle provide international administrative assistance, but, unlike Convention 108+, does not establish legally binding obligations for the participating authorities but is of voluntary nature.

II. United Nations

The protection of personal data also plays a major role at the level of the UN. In addition to the UDHR and the International Bill of Rights, the further development of the UN’s attitude to the protection of personal data was primarily driven by its “guidelines” and “resolutions”. At the UN, transborder data flows are also named as a problem area, which necessarily goes hand in hand with globalization, but for which a legal framework is still largely lacking, according to a 2013 report of the Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion.¹²⁵⁴ The work on UN Guidelines was rooted primarily on human rights concerns. It repeated and strengthened a 22-year lasting approach to data protection, beginning with a General Assembly Resolution in 1968¹²⁵⁵. Later, the “Resolution on the right to privacy in the digital age”

¹²⁴⁹ Greenleaf, G. [Graham] and Clarke, R. [Roger] and Waters, N. [Nigel]. (27 September 2013). International Data Privacy Standards: A Global Approach (Australian Privacy Foundation Policy Statement), *UNSW Law Research Paper* No. 2013-62, <http://dx.doi.org/10.2139/ssrn.2327325>. P. 3.

¹²⁵⁰ Greenleaf, G. [Graham] and Clarke, R. [Roger] and Waters, N. [Nigel]. (27 September 2013). International Data Privacy Standards: A Global Approach (Australian Privacy Foundation Policy Statement), *UNSW Law Research Paper* No. 2013-62, <http://dx.doi.org/10.2139/ssrn.2327325>. P. 3.

¹²⁵¹ OECD. *Action Plan for the Global Privacy Enforcement Network (GPEN)*, <https://www.privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen>, (15 June 2012). // Part E of GPEN has been amended on 22 January 2013.

¹²⁵² OECD. *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352>, (6 December 2007).

¹²⁵³ Global Privacy Enforcement Network. (23 July 2023). *Members*. <https://www.privacyenforcement.net/content/members>.

¹²⁵⁴ The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, stated that national laws that regulate the involvement of states in communication surveillances often do not exist, or are inadequate and also highlighted the link between general privacy protections (including those for informational privacy) and other rights. // See UN, General Assembly. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40*, (17 April 2013). P. 3, 6–8.

¹²⁵⁵ UN, General Assembly. *Human rights and scientific and technological developments, Resolution 2450 of 19 December 1968, E/CN.4/1025*, (19 December 1968).

(Resolution 2013)¹²⁵⁶ emphasized the scope of technological change, the importance of data protection and the dangers posed by State surveillance.

1. Universal Declaration of Human Rights

The UDHR was the first international instrument to standardize the right to privacy in Art. 12 UDHR, which reads: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.” The question is to whom this responsibility is directed. The traditional view of international law is that this is a law concerning State relations and conduct. According to this, only the conduct of a State could give rise to a responsibility under international law, no other actor could violate these obligations, and the State would have no positive obligations with respect to fundamental rights. However, international human rights law has evolved over the years in this regard. For this development, the preamble of the UDHR gave way by promulgating that the UDHR was “a common standard of achievement for all peoples and all nations” and obligating every individual and every organ of society “to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance”. This suggests that States have also the obligation to take positive steps to ensure the enjoyment of human rights. The right to privacy in the UDHR can therefore be understood in two ways: a duty to protect and a right of defense.

Art. 12 UDHR prohibits “arbitrary” interference with the right to privacy by a State or by another individual, which follows from the general right to liberty in Arts. 1 and 3 UDHR.¹²⁵⁷ Accordingly, such interference is only permissible if it occurs based on a law that in turn describes conditions for just non-arbitrary interference. Art. 12 UDHR also requires a guarantee by a State for everyone to obtain legal protection against a violation of his or her right to privacy.

The concept of “privacy” is understood broadly here as well, its manifestations also include the protection of personal sphere (e.g., intimate personal relationships or activities, fundamental choices of the individual involving himself, his family, and his relationships with others)¹²⁵⁸ and personal data. Since the scope of Art. 12 follows from Arts. 1 and 3 UDHR, the enumeration of protected rights in Art. 12 UDHR is not to be understood as exhaustive. Moreover, the protection of honor and reputation in the UDHR point to, that, on the one hand, the personality, and on the other hand, that the social perception of a person are included in the scope of Art. 12 UDHR. Transferring this idea to the present day, it seems logical to also protect the personality online.

The UDHR provides that the right to privacy is subject to the limitations in Art. 29 UDHR. Individuals thus have duties to their fellow human beings and to the community to which they belong and are called upon to work for the promotion of and respect for the rights recognized in the UDHR. Art. 29(2) UDHR allows States to impose legal restrictions on the rights and freedoms of the UDHR, but only for specific and expressly stated purposes. The protection of privacy must therefore not be abused to undermine other human rights - such as the right to freedom of expression in Art. 19 UDHR. The term

¹²⁵⁶ UN, General Assembly. *Resolution adopted by the General Assembly on 18 December 2013, A/RES/68/167*, (18 December 2013). (“Resolution 2013”).

¹²⁵⁷ USA. *IND. FOUNDATION, ETC. v. Texas Ind. Acc. Bd.*, Supreme Court of Texas, 540 S.W.2d 668 (1976). P. 679: “It is apparent from the above that the term “right of privacy” is actually a generic term encompassing various rights recognized by the Court to be “inherent in the concept of ordered liberty.”

¹²⁵⁸ Similar in USA. *IND. FOUNDATION, ETC. v. Texas Ind. Acc. Bd.*, Supreme Court of Texas, 540 S.W.2d 668 (1976). P. 679.

“democratic society” is understood here as referring to morality, public order and the common good. However, what constitutes a “democratic society” remained undefined. Art. 30 UDHR provides a norm to interpret the UDHR by regulating that no one should be allowed to invoke the UDHR who wants to abolish the rights it protects. This abuse clause thus also limits Art. 29 UDHR, which States may wish to invoke under the conditions stated therein.

2. International Bill of Human Rights

Together with the UDHR, the ICCPR and the “International Covenant on Economic, Social and Cultural Rights” (ICESCR)¹²⁵⁹ comprise what is known as the “International Bill of Human Rights”. Both covenants proclaim these rights for all people and forbid discrimination. Unlike the UDHR, both are binding international conventions for their Parties. The ICCPR focuses on issues such as the right to life, freedom of speech, religion, and voting; the ICESCR on food, education, health, and shelter and is therefore not of interest for the matter of this thesis. The ICCPR represents an essential part of international law. All Parties to the US framework¹²⁶⁰ and European framework have ratified it. The discussion about data protection within the UN was dominated by full consensus that the right to data protection must be anchored in the ICCPR, which shows that the Parties consider data protection as a universal human right and recognize it as a common approach behind the different protected legal interests in Art. 17 ICCPR.¹²⁶¹

Art. 2(1) ICCPR requires State Parties “to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant”. Each party shall provide in accordance with Art. 2(3) ICCPR effective remedies for violations of the ICCPR. The provisions of Art. 2 ICCPR therefore suggest “that this duty has two limbs. The first is the duty take preventive measures against occurrence of violations of human rights by private actors. The second is the duty to take remedial measures once the violations have occurred”¹²⁶².

Art. 17 ICCPR contains an almost same formulation as Art. 12 UDHR, with almost identical protected goods: “privacy, family, home, correspondence, honor and reputation”. Art. 17 ICCPR guarantees everyone protection against interference with private life. This also includes the right to informational self-determination; it is therefore the relevant provision for the protection of personal data. The main difference to Art. 12 UDHR is the inclusion of the term “unlawful” in Art. 17 ICCPR, which means a certain weakening of protection compared to Art. 12 UDHR. Art. 17 ICCPR rendered data protection legally binding in international law. It has also similarities to Art. 11 of the “Inter-American Commission on Human Rights”.¹²⁶³ The protection of privacy and correspondence is also enshrined in Art. 21 of the “Arab Charter on Human Rights”¹²⁶⁴. Only the “African Charter on Human’s and People’s Rights” does not explicitly recognize

¹²⁵⁹ UN, Office of the High Commissioner for Human Rights. *International Covenant on Economic, Social and Cultural Rights*, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>, (16 December 1966).

¹²⁶⁰ Nevertheless, “many countries have elected to make certain reservations, understandings, and declarations (“RUDs”). None of the countries have made more RUDs than the United States. [...] [to the US’s RUDs] objecting countries were Belgium, Denmark, Finland, France, Germany, Italy, The Netherlands, Norway, Portugal, Spain, and Sweden”. // See Ash, K. [Kristina]. (2005). U.S. Reservations to the International Covenant on Civil and Political Rights: Credibility Maximization and Global Influence. *Northwestern Journal of International Human Rights*, 3(1), Article 7. P. 3–4. // Although the US did not raise RUDs against Art. 17 ICCPR, it is significant that the US made declarations regarding the treaty being non-self-Executing, saying that the treaty does not create a private cause of action in the US.

¹²⁶¹ UN, General Assembly. *Doc. A/2929*, (1 July 1955). P. 46.

¹²⁶² Chirwa, D. [Danwood]. (2019). State Responsibility for Human Rights. In M. [Manisuli] Ssenyonjo, *International Human Rights Law. Six Decades after the UDHR and Beyond* (pp. 397–410). Routledge. P. 405.

¹²⁶³ Inter-American Specialized Conference on Human Rights. *American Convention on human rights*, (22 November 1969).

¹²⁶⁴ UN, Office of the High Commissioner for Human Rights. *Arab Charter on Human Rights*, <https://digitallibrary.un.org/record/551368>, (2004).

the protection of privacy.¹²⁶⁵ More problematic is the effect of the absence of a binding human rights agreement in APAC, since several APAC countries, especially China, have signed but not yet ratified the ICCPR.

The ECtHR can also include the practice of the UN HRC on Art. 17 ICCPR. There are parallels between the opinions of the ECtHR on the one hand, and the UN HRC on Art. 17 ICCPR on the other. The wording of Art. 17 ICCPR and Art. 8 ECHR protect the same aspects, defensive rights as well as obligations to protect individuals can be derived from both instruments. Similarities also exist in the interpretation of the protected aspects. Thus, the dynamic interpretation through both the UN HRC and the ECtHR have extended the level of protection.

Arts. 28 ff. ICCPR regulate the composition and functions of the UN HRC, which monitors compliance with the ICCPR. The UN HRC does have the opportunity to other interpretations whenever new developments appear. This takes place by the fact that the UN HRC supersedes or supplements existing “General Comments”¹²⁶⁶ where necessary to develop the content of protected rights, and to reflect changing realities. The UN HRC made use of this possibility in 1988 when it issued “General Comment 16”¹²⁶⁷ and hereby interpreted Art. 17 ICCPR. This is the only General Comment to date regarding Art. 17 ICCPR. This Comment focused on the obligation of States to use regulatory instruments to protect their citizens’ personal data by stating that “this right is required to be guaranteed against all [...] interferences and attacks whether they emanate from State authorities or from natural or legal persons”. The term “legal persons” is “clearly intended to mean business and consequently obliges States to guarantee the protection of user data by technology companies under their jurisdiction”¹²⁶⁸. Art. 17 ICCPR thus also includes a defense right and a duty to protect. This duty to protect implicitly also covers the obligation to control and regulate private actors. Comment 16 on Article 17 ICCPR stipulated on that aspect that

the gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person’s private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data are stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public [authorities] or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.¹²⁶⁹

¹²⁶⁵ African Commission on Human and Peoples' Rights. *African Charter on Human and Peoples' Rights*, (27 June 1981).

¹²⁶⁶ “Each of the treaty bodies publishes its interpretation of the provisions of its respective human rights treaty in the form of “general comments” or “general recommendations”.” See UN, Office of the High Commissioner for Human Rights. (23 July 2023). *Human Rights Treaty Bodies - General Comments*. <https://www.ohchr.org/en/hrbodies/pages/tbgeneralcomments.aspx>.

¹²⁶⁷ UN. *Compilation of General Comments and General Recommendations adopted by human rights treaty bodies*, HRI/GEN/1/Rev.1, (29 July 1994). P. 21–23.

¹²⁶⁸ Perry, S. [Susan] and Roda, C. [Claudia]. (2017). *Human Rights and Digital Technology*. Palgrave Macmillan. P. 71.

¹²⁶⁹ UN. *Compilation of General Comments and General Recommendations adopted by human rights treaty bodies*, HRI/GEN/1/Rev.1, (29 July 1994). P. 21–23. Para. 10.

States have therefore also a duty to provide a legislative framework prohibiting acts constituting arbitrary and unlawful interference with the right to data protection by natural and legal persons.

The UN HRC has also made clear, that the term “correspondence” should be interpreted broadly and covers not only the traditional letter or communications traffic, but also modern electronic means of communication. It also emphasized that the protection of personal data from a human rights perspective is part of the right to privacy and freedom of correspondence.¹²⁷⁰ In her report to the Resolution 2013, the former UN High Commissioner for Human Rights, Navi Pillay, found that any form of interference in the communication process, even if it is collecting aggregated data (Big Data) acts as interference with the right to privacy.¹²⁷¹ State surveillance measures would only be legitimate under international law if they comply with the human rights requirements of Art. 17 ICCPR.¹²⁷² The report also emphasized that the right to data protection is threatened not only by targeted government investigations, but increasingly by “voluntary” disclosure of personal data on the Internet.¹²⁷³

Interference with the rights under Art. 17 ICCPR must be:

- a. Carried out pursuant to the requirements of domestic and international law, including the provisions, aims and objectives of the ICCPR;
- b. Authorized by laws that the public can fully access, and that are precise, specific, and clearly defined such that an impacted individual can foresee any interference;
- c. Necessary for and proportionate to the pursuit of legitimate State aims, such as law enforcement or national security;
- d. Minimally intrusive of protected privacy interests, and in any event, never so invasive as to impair the essence of the right.¹²⁷⁴

The protected rights under Art. 17 ICCPR and supranational human rights conventions in a certain region are nevertheless not absolute.¹²⁷⁵ According to the practice of the UN HRC, interventions are justified if they are made on a legal basis and the statutory objectives are compatible with purpose and aim of the ICCPR. Art. 19(3b) ICCPR plays an important role for the Parties in this respect. Parts of US literature had considered that the operational controls of the NSA were justified by this Article.¹²⁷⁶ Such measures of interference must nevertheless undergo a proportionality test¹²⁷⁷. Judicial review and control must be accessible, Art. 17(2) ICCPR.

¹²⁷⁰ Nowak, M. [Manfred]. (2005). *UN Covenant on Civil and Political Rights. CCPR Commentary*. Engel. P. 401

¹²⁷¹ UN, HRC. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*, (30 June 2014). Paras. 18 and 19.

¹²⁷² UN, HRC. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*, (30 June 2014). Para. 15.

¹²⁷³ UN, HRC. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*, (30 June 2014). Para. 18.

¹²⁷⁴ ACLU. (February 2015). *Informational Privacy in the Digital Age, A Proposal to Update General Comment 16 (Right to Privacy) to the International Covenant on Civil and Political Rights, A Report by the American Civil Liberties Union*. https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf. P. ii.

¹²⁷⁵ UN. *Compilation of General Comments and General Recommendations adopted by human rights treaty bodies*, HRI/GEN/1/Rev.1, (29 July 1994). P. 21–23. Para. 7.

¹²⁷⁶ Margulies, P. [Peter]. (2014). The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism. *Fordham International Law Review*, 82(5), 2137–2167. P. 2152 ff.

¹²⁷⁷ “the Special Rapporteur takes the position that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, as elucidated in General Comment 27. The test as expressed in the comment includes, inter alia, the following elements: (a) Any restrictions must be provided by the law (paras. 11–12); (b) The essence of a human right is not subject to restrictions (Para. 13); (c) Restrictions must be necessary in a democratic society (Para. 11); (d) Any discretion exercised when implementing the restrictions must not be unfettered (Para. 13); (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim (Para. 14); (f) Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected

Art. 17 ICCPR constitutes the basis for the United Nations' protection of personal data from a human rights perspective. However, the little concrete formulation of Art. 17 ICCPR still troubles the UN HRC to set specific requirements for Parties' national legislation. The protective measures are therefore within the discretion of the individual Parties. This led, through the influencing factors of the 9/11 attacks and the NSA affair, to disagreements among the Parties. After the NSA affair, the German government wanted the right to data protection to be strengthened in the ICCPR through an announcement by the former German Chancellor¹²⁷⁸ and a letter by the German Ministry of Foreign Affairs and Justice¹²⁷⁹ sent to the ministers of the EU countries. The "American Civil Liberties Union" (ACLU) also noted that this "General Comment does not fully address State responsibilities surrounding privacy in the digital age [... and] at minimum, an update to General Comment 16 is necessary to reaffirm the continued relevance of human rights principles to current surveillance practices"¹²⁸⁰ and called for the following improvements:

a. Indiscriminate mass surveillance, including mass collection and retention of data, violates Article 17 because it is an unlawful and typically arbitrary interference with informational privacy; b. Both metadata and communications content may trigger the protections of Article 17; c. Any interference with informational privacy should be subject to independent and effective oversight; d. In relation to privacy rights, it is control over communications or relevant infrastructure, not custody of the person, that is the touchstone of State responsibility; e. Laws on privacy and surveillance must not be discriminatory, and in particular, must not distinguish between people simply on the grounds of nationality; instead, differential treatment is only permissible when based also on acceptable grounds under the Covenant, and when there is a reasonable, objective purpose for drawing the distinction, and doing so supports a legitimate aim; and f. States Parties have affirmative obligations to protect informational privacy from interference by private Parties and other States, and to ensure effective remedies for victims of privacy breaches.¹²⁸¹

It remains to be seen when the UN HRC will react to the developments with a revision or complete replacement of its General Comment 16. Especially since other instruments of the UN system have already reacted to this development through, e.g., Resolution 2013, Resolution 2021, and the reports by the Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion.

(paras. 14-15)." // See UN, General Assembly. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40*, (17 April 2013). P. 8–9.

¹²⁷⁸ "As the lead ministry, the Federal Foreign Office is working at international level to negotiate an additional protocol to Article 17 of the ICCPR. The content of such an additional protocol - which would, incidentally, be the third additional protocol - is to be supplementary international agreements on data protection that reflect today's modern technical developments and also cover the activities of intelligence services. A joint initiative to our European partners was taken today by the Federal Foreign Minister together with the Federal Minister of Justice in the form of a letter to obtain a common European position on this issue." // See Die Bundesregierung. (19 July 2013). *Sommerpressekonferenz von Bundeskanzlerin Merkel vom 19. Juli*. <https://www.bundeskanzler.de/bk-de/suche/sommerpressekonferenz-von-bundeskanzlerin-merkel-vom-19-juli-844124>.

¹²⁷⁹ "The existing human rights provisions, in particular Article 17 of the International Covenant on Civil and Political Rights, date back to a long time ago. However, this provision can be seen as the human rights starting point for international data protection. It is therefore a suitable starting point for supplementary international agreements on data privacy that are up-to-date and in line with modern technical developments. Our goal should therefore be to supplement the ICCPR with an additional protocol to Article 17, that safeguards the protection of privacy in the digital age. To this end, we intend to seek a Conference of the Parties." // See Auswärtiges Amt und Bundesministerium der Justiz. (19 July 2013). *Letter of 19 July 2013*. https://cdn.netzpolitik.org/wp-upload/2013-07-19_AA_BMJ_Aussen_Justiz.pdf.

¹²⁸⁰ ACLU. (February 2015). *Informational Privacy in the Digital Age, A Proposal to Update General Comment 16 (Right to Privacy) to the International Covenant on Civil and Political Rights, A Report by the American Civil Liberties Union*. https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf. P. ii, 2.

¹²⁸¹ ACLU. (February 2015). *Informational Privacy in the Digital Age, A Proposal to Update General Comment 16 (Right to Privacy) to the International Covenant on Civil and Political Rights, A Report by the American Civil Liberties Union*. https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf. P. ii.

3. Guidelines for the Regulation of Computerized Personal Data Files

The UN Guidelines are intended for all Member States of the UN and therefore have a wide geographical reach. They are non-binding under international law and, like the OECD Guidelines 1980 and 2013, have the character of a guideline.¹²⁸² Their scope is aimed primarily at “computerized data files”. The term “computerized” covers not only data on personal computers, but also the data stored on other computer-based systems. Following the example of the OECD Guidelines 1980, the UN Guidelines encompass both the public and the private sector, and also international organizations. For purposes of control, the law of each Member State shall determine an independent body which monitors compliance with the UN Guidelines in accordance with its domestic law.

Art. 9 UN Guidelines stresses the importance of a free TFPD and suggests a trade-off in terms of a proportionality test:

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

Compared to Convention 108 and the OECD Guidelines 1980, the UN Guidelines thus employed slightly different formulations of the criteria for restricting such flows. “Comparable and reciprocal are more diffuse and confusing than the criterion of equivalent protection used in the CoE Convention [108] and OECD [1980] Guidelines”¹²⁸³.

With the UN Guidelines, a first consensus at global level was reached on certain principles of data protection law. In contrast to Convention 108 and the OECD Guidelines 1980, the UN Guidelines encouraged international organizations to process personal data in a privacy-friendly manner and introduced the principle of accuracy.

Nevertheless, only 13 Member States complied with the request of the Human Rights Commission to report to the Secretary General on measures they have taken to implement the UN Guidelines. The current provisions are characterized by general clauses and abstract terminology. “Personal data” and “personal data file”, e.g., remained undefined. Although “comparable safeguards” is a prerequisite for the transfer of personal data between Member States, this term is not defined more precisely. The UN Guidelines can thus not provide a sufficiently differentiated standard for handling data to be relevant in practice, which is last not least also underlined by the small quantity of materials by researchers and practitioners on the UN Guidelines. The UN Guidelines are therefore of even less practical importance than the Convention 108 and the OECD Guidelines 2013.¹²⁸⁴

¹²⁸² The preamble of the UN Guidelines states: “The procedures for implementing regulations concerning computerized personal datafiles are left to the initiative of each State subject to the following orientations.”

¹²⁸³ Bygrave, L. A. [Lee A.]. (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar. P. 30.

¹²⁸⁴ Fischer, P. E. [Philipp Eberhard]. (2012). Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing. *JIPITEC*, 3(1), 33–59. <https://www.jipitec.eu/issues/jipitec-3-1-2012/3321/fischer.pdf>. P. 46.

4. Resolution on the right to privacy in the digital age, and others within the UN system

Unlike a UN Security Council resolution, a resolution such as Resolution 2013 by the UN General Assembly is not binding under international law. Nevertheless, its symbolic and political value is substantive. With the concentrated power of the approval of all UN Member States in the General Assembly behind it, its symbolic effect should not be underestimated. Since General Assembly resolutions are regularly supported by a significantly larger number of States, they are not legally meaningless but generally fall under the heading of “soft law”. Whether soft law develops into international custom over time, as mentioned above¹²⁸⁵, depends on the practice of States (*consuetudo*) and corresponding legal conviction (*opinio iuris*) that underpin it.

In Resolution 2013 the UN called upon States “to establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance or communications, their interception and the collection of personal data”¹²⁸⁶. Even States, whose practices were the reason for this document, agreed to Resolution 2013. These include the US, which had been criticized for spying on foreign citizens,¹²⁸⁷ but also countries such as Russia and North Korea, which are still criticized today for monitoring their own citizens. For the first time in the history of the UN, the protection of privacy, as for example enshrined in the secrecy of letters and e-mail communication, was also enshrined for online communication.¹²⁸⁸ Resolution 2013 was therefore an important step in the expansion of human rights in the digital age. Before finding compromise on the final version, the wording was controversial regarding rules of the ICCPR, especially whether the ICCPR shall be applied to activities of government authorities outside of their own territory, for example, for intelligence activities abroad. The terms “its territory” and “subject to its jurisdiction” in Art. 17 ICCPR are understood by the US and Israel as cumulative requirements.¹²⁸⁹ However, both the ICJ and the UN HRC, which is responsible for monitoring the guarantees of the ICCPR, have affirmed that the obligations of the ICCPR apply beyond their own territories.¹²⁹⁰ As a result of this disagreement, Resolution 2013 no longer speaks of the fact that human rights violations can result from extraterritorial telecommunications surveillance. Rather, the final version included only that such measures can have negative consequences for the exercise of human rights. This could enable opponents of an extraterritorial application of the ICCPR to maintain their legal position. The negotiations on the Resolution 2013 showcase how difficult it can be to reach an international human rights treaty that does not fall below the already existing level of data protection. Nevertheless, by referring to ICCPR rights, Resolution 2013 reaffirmed the limits for action by intelligence agencies and underlined that this also applies to the fight against terrorism. The 2013 resolution called on all Member States to respect the data protection rights and to put an end to any violations.

¹²⁸⁵ Chapter I, Section II.5.5.

¹²⁸⁶ UN, General Assembly. *Resolution adopted by the General Assembly on 18 December 2013*, A/RES/68/167, (18 December 2013). Para. 6.d.

¹²⁸⁷ Ultimately, however, neither the US as such nor the NSA were explicitly named, and room for interpretation was left as to when surveillance measures violate human rights.

¹²⁸⁸ UN, General Assembly. *Resolution adopted by the General Assembly on 18 December 2013*, A/RES/68/167, (18 December 2013). Para. 3.

¹²⁸⁹ UN, Human Rights Committee. *Comments on United States of America*, CCPR/C/79/Add 50, (1995). Para. 19. // UN, Human Rights Committee. *Consideration of reports submitted by States parties under article 40 of the Covenant*, CCPR/C/ISR/CO/3, (2010). Para. 5.

¹²⁹⁰ ICJ. (9 July 2004). *Reports of judgments, advisory opinions and orders, Legal consequences of the construction of a wall in the occupied Palestinian territory*. <https://www.icj-cij.org/public/files/case-related/131/131-20040709-ADV-01-00-EN.pdf>. Para 111. // UN, HRC. General Comment No. 31 (80). The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13, (26 May 2004). Para. 10

Independent monitoring mechanisms are to be introduced to establish transparency and accountability regarding State activities.

With Resolution 2013, the UN reaffirmed the “Vienna Declaration and Programme of Action”¹²⁹¹ which confirmed in Para. 1 the universality of human rights by stating that “the solemn commitment of all States [is] to fulfil their obligations to promote universal respect for, and observance and protection of, all human rights and fundamental freedoms for all in accordance with the Charter of the United Nations, other instruments relating to human rights, and international law. The universal nature of these rights and freedoms is beyond question.”

Resolution 2013 was followed by a detailed report of the High Commissioner for Human Rights on the right to privacy in the digital age.¹²⁹² The report concluded that “practices in many States have [...] revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy”. In 2015, the UN HRC requested its first “Special Rapporteur on the right to privacy” to “seek credible and reliable information from Governments, non-governmental organizations and any other Parties who have knowledge of situations and cases relating to privacy”¹²⁹³. On 17 December 2018, the UN General Assembly adopted Resolution A/RES/73/179¹²⁹⁴, noting that women as well as children, are particularly vulnerable to violations and abuses of the right to privacy. On 23 September 2019, 27 nations signed a joint resolution at the UN General Assembly to promote responsible behavior in cyberspace.¹²⁹⁵ Co-signatories include Germany, the US, France, and the UK. Russia and China are not signatory States. This resolution states that the signatories have a responsibility to keep cyberspace free, open, and secure for future generations. Countries that violate that resolution would be liable under international law. The resolution states that

UN member states have increasingly coalesced around an evolving framework of responsible state behavior in cyberspace (framework), which supports the international rules-based order, affirms the applicability of international law to state-on-state behavior, adherence to voluntary norms of responsible state behavior in peacetime, and the development and implementation of practical confidence building measures to help reduce the risk of conflict stemming from cyber incidents. All members of the United Nations General Assembly have repeatedly affirmed this framework, articulated in three successive UN Groups of Governmental Experts reports in 2010, 2013, and 2015.

With this resolution, the Member States thus fostered their commitment to an international rules-based order for Cyberspace.

Resolution 2013 not only opposed surveillance, but also called for a UN report on the impact of surveillance. The High Commissioner for Human Rights commented in 2021 “how the widespread use by States and businesses of artificial intelligence, including profiling, automated decision-making and machine-learning technologies, affects the

¹²⁹¹ UN, HRC. *Vienna Declaration and Programme of Action*, <https://www.ohchr.org/sites/default/files/vienna.pdf>, (25 June 1993).

¹²⁹² UN, HRC. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*, (30 June 2014).

¹²⁹³ UN, Office of the High Commissioner for Human Rights. (2023). *Special Rapporteur on the right to privacy*. <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

¹²⁹⁴ UN, General Assembly, “The right to privacy in the digital age”, 21 January 2019, A/RES/73/179

¹²⁹⁵ German Federal Foreign Office. (24 September 2022). *Shaping Global Cybersecurity - A Call for Action to Promote Responsible State Behavior and Capacity-Building*. <https://www.auswaertiges-amt.de/en/newsroom/news/-/2554280>.

enjoyment of the right to privacy and associated rights”.¹²⁹⁶ This was reaffirmed on 7 October 2021 in a resolution adopted by the HRC (Resolution 2021)¹²⁹⁷, wherein the UN built on the language of previous UN resolutions; in particular, it

- recognizes that metadata can reveal information as sensitive as content data;
- recognizes that the use of artificial intelligence can pose serious risks to the right to privacy, in particular when employed for identification, tracking, profiling, facial recognition, behavioral prediction or the scoring of individuals;
- recommends states to ensure that facial recognition technologies by public and private actors do not enable arbitrary or unlawful surveillance, including of those exercising their right to freedom of peaceful assembly; and
- calls on states not to limit access to encryption technologies and anonymity tools.¹²⁹⁸

III. World Trade Organization

The “World Trade Organization” (WTO) is a global organization “related to the UN”. It has “no reporting obligation to the GA [General Assembly] but on an ad hoc basis to GA and Economic and Social Council (ECOSOC) work on, inter alia, finance and development issues”¹²⁹⁹. Its rules apply to all major business centers, such as China, the EU and its Member States, and the US. In the field of public international law, WTO law forms an autonomous jurisdiction, which is enforced through the WTO Dispute Settlement System. 86 WTO Member States represent over 90% of global trade.¹³⁰⁰ As the following graphic shows, all countries significantly involved in the global digital economy are also members of the WTO.



Source: WTO, “Members and Observers”¹³⁰¹

¹²⁹⁶ UN, Office of the High Commissioner for Human Rights. *The right to privacy in the digital age: report (2021)*, A/HRC/48/31, (13 September 2021). P. 1.

¹²⁹⁷ UN, General Assembly. *Resolution adopted by the Human Rights Council on 7 October 2021*, A/HRC/RES/48/4, (13 October 2021). (“Resolution 2021”).

¹²⁹⁸ Privacy International. (14 December 2022). *Recognition of Privacy in UN Human Rights Mechanisms*. <https://privacyinternational.org/privacy-un-human-rights-mechanisms>.

¹²⁹⁹ UN. (July 2021). *The UN System Chart*. https://www.un.org/en/pdfs/un_system_chart.pdf.

¹³⁰⁰ OECD. (12 October 2022). *Cross-border Data Flows. Taking Stock of Key Policies and Initiatives*. <https://www.oecd.org/publications/cross-border-data-flows-5031dd97-en.htm>. P. 10.

¹³⁰¹ WTO. (23 July 2023). *Members and Observers*. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm. // Green: WTO Member States; Yellow: Observers negotiating accession; Grey: States without official relations with the WTO.

The discussion on E-Commerce in the WTO began in May 1998 with a declaration.¹³⁰² Since then, a work program based on this declaration envisaged to study all trade-related issues of E-Commerce. Since 2019, 71 countries were negotiating an agreement under the umbrella of the WTO to create rules for global E-Commerce (WTO JSI).¹³⁰³ The need for such negotiations stems from the fact that since 1998, a wide variety of free trade agreements have evolved into forums for the governance of the digitization of transborder trade relations. In view of an increasing drifting apart from different region-based models, the WTO JSI has been negotiating common rules for E-Commerce. “E-Commerce” in this respect refers not only to traditional online trade, but also the duty-free treatment of electronic transfers as well as sectoral issues such as TFPD.

In a joint statement, 42 digital and consumer protection organizations from around the world called for fundamental data protection rights to be safeguarded in those negotiations.¹³⁰⁴ Therein, the organizations explicitly supported the positioning of the EU and demanded:

If “cross-border data flows” rules are part of the future WTO agreement: To upgrade the existing safeguards, putting people’s data protection and privacy rights first so that the digital economy can thrive and consumers’ trust is regained. If these conditions cannot be met: To exclude or not to commit to rules on cross-border data flows from the negotiations and final deal. Endorsing other binding international rules – notably Convention 108+ for the Protection of Individuals with Regard to the Processing of Personal Data – will be more balanced. 55 countries have become Parties to Convention 108 already.¹³⁰⁵

The EU’s negotiating mandate provides for addressing the area of TFPD in those negotiations. It is in the EU’s interest to anchor the most ambitious regulations possible in the area of data flows, while at the same time respecting European values and fundamental rights, such as the protection of personal data. The EU’s position also implies that, firstly, possible initiatives by countries to provide for local data storage contradict the position taken by the EU on data flow restrictions, and, secondly, that the EU may not agree to obligations that could affect its existing legal framework for the protection of personal data.

A draft consolidated negotiating text shows that the US and China have opposing approaches on the issue of regulating TFPD, while the EU’s negotiating position is positioned between these two extremes.¹³⁰⁶ Thus, the positions of the US and the EU clash in the area of tension between free TFPD and the reservations of national data protection regulations. In the meantime, 86¹³⁰⁷ countries have been involved in the negotiations; among them, there is a class division between more developed and less developed countries, which led to criticism.

¹³⁰² WTO. *Declaration on Global Electronic Commerce*, WT/MIN(98)/DEC/2, (25 May 1998).

¹³⁰³ WTO. (4 April 2023). *Joint Initiative on E-commerce*.

https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm.

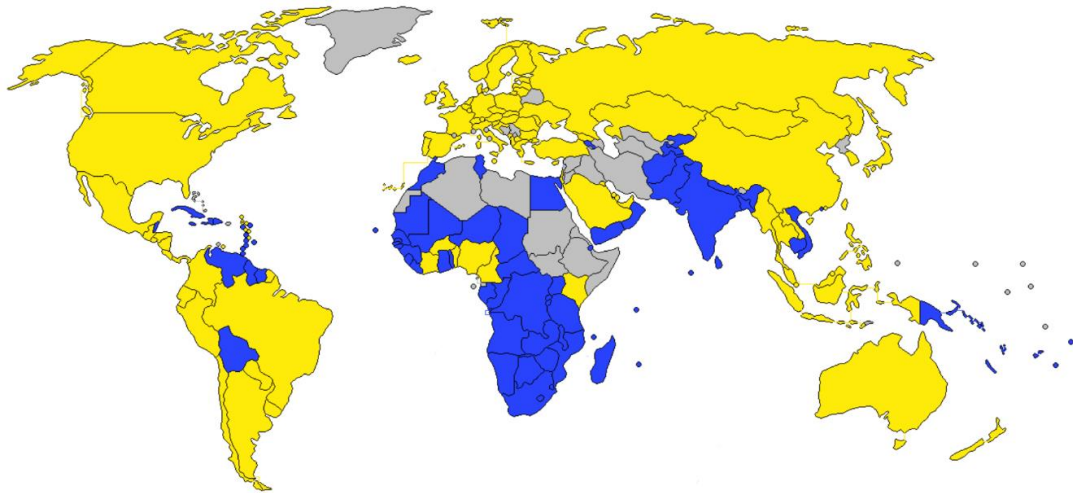
¹³⁰⁴ The European Consumer Organization. (16 November 2020). *WTO trade talks must safeguard privacy, 42 organizations urge*. <https://www.beuc.eu/news/wto-trade-talks-must-safeguard-privacy-42-organisations-urge>.

¹³⁰⁵ WTO. *Joint Statement on Electronic Commerce. EU proposal for WTO disciplines and commitments relating to Electronic Commerce*, INF/ECOM/22, (26 April 2019).

¹³⁰⁶ WTO. *Electronic Commerce Negotiations, Consolidated Negotiating Text*, INF/ECOM/62/Rev.1, (14 December 2020).

¹³⁰⁷ As of February 2023, there are now 89 WTO members participating in these discussions, accounting for over 90 per cent of global trade. // WTO. (4 April 2023). *Joint Initiative on E-commerce*.

https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm.



Source: Netzpolitik.org, "Digitalwirtschaften ärmerer Länder sollen weiter schutzlos bleiben"¹³⁰⁸

Topics such as E-Commerce are complex and fewer developed Members of these negotiations "have rather limited capacities to engage in negotiations: our delegations [delegation of Côte d'Ivoire] in Geneva are quite small and our officials have various obligations outside the WTO. We cannot afford to send experts to cover all areas of negotiation. We cannot afford to draw on technical support from our capitals as the more advanced countries are able to do. It is therefore understandable that we focus our limited resources on matters of importance to our countries and that we have difficulty tackling subjects as complex as e-commerce".¹³⁰⁹ The delegation of Côte d'Ivoire also expressed an understandable concern that "an isolated agreement on e-commerce without progress on multilateral issues of importance could compromise the inclusive multilateral system"¹³¹⁰. UNCTAD had also expressed concern that a hasty liberalization of digital trade could have a negative impact on building the digital economy in the Global South.¹³¹¹

At a joint press conference held in December 2021, a WTO Joint Statement by Ministers of Australia, Japan and Singapore has been published. It pointed out that the WTO JSI "achieved good convergence in negotiating groups on eight articles – online consumer protection; electronic signatures and authentication; unsolicited commercial electronic messages; open government data; electronic contracts; transparency; paperless trading; and open internet access. [...] We will intensify negotiations in these areas from early 2022. We note that provisions that enable and promote the flow of data are key to high standard and commercially meaningful outcome."¹³¹² While an agreement could presumably be reached quickly on the technical rules for E-Commerce, it remains to be seen what progress will be made in the negotiations during the 12th WTO Ministerial Conference in June 2022¹³¹³.

¹³⁰⁸ Henning, M. [Maximilian]. (9 March 2021). *Digitalwirtschaften ärmerer Länder sollen weiter schutzlos bleiben*. <https://netzpolitik.org/2021/verhandlungen-bei-der-wto-digitalwirtschaften-aermerer-laender-sollen-weiter-schutzlos-bleiben>. // Yellow: Member of the e-commerce negotiations; Blue: WTO member and no Member of the e-commerce negotiations; Gray: Not a (full) WTO Member.

¹³⁰⁹ WTO. *Joint statement on electronic commerce - Communication from Côte d'Ivoire*, INF/ECOM/4, (16 December 2019). P. 2.

¹³¹⁰ WTO. *Joint statement on electronic commerce - Communication from Côte d'Ivoire*, INF/ECOM/4, (16 December 2019). P. 2.

¹³¹¹ UNCTAD. *Rising Product Digitalization and Losing Trade Competitiveness*, UNCTAD/GDS/ECIDC/2017/3, (2017). P. 17–18.

¹³¹² WTO. (December 2021). *WTO Joint Statement Initiative on E-commerce. Statement by Ministers of Australia, Japan and Singapore*. https://www.wto.org/english/news_e/news21_e/ji_ecom_minister_statement_e.pdf.

¹³¹³ The "substantial progress by the 12th WTO Ministerial Conference" which WTO JSI promises on their website has not yet been made available to the public. // WTO. (4 April 2023). *Joint Initiative on E-commerce*. https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm.

Until then, the existing WTO rules remain important for this thesis. The legal system of the WTO is based on the three pillars of trade in goods, trade in services and intellectual property rights. These are laid down in the multilateral trade agreements that apply to all Members: The “General Agreement on Tariffs and Trade” (GATT)¹³¹⁴, the “General Agreement on Trade in Services” (GATS)¹³¹⁵ and the “Agreement on Trade-Related Aspects of Intellectual Property Rights” (TRIPS)¹³¹⁶.

A cornerstone of the WTO regime is the distinction between goods and services.¹³¹⁷ Goods are governed by GATT, while services are governed by GATS. Although the WTO includes “data processing” in its “Services Sectoral Classification List” among “CPC Division 84 - Computer and Related Services”¹³¹⁸, it has yet not decided explicitly whether TFPD are to be classified as trade in goods or trade in services. This complicates legal certainty because

commitments and obligations differ under each agreement and thus assessing the legality of a specific measure is complex. For instance, under GATT rules, national treatment is automatically extended while in the GATS, national treatment is a negotiated commitment¹³¹⁹ which differs across country and sector. [...] If considered under the GATT, the legality of the data measure will depend on whether there is an alternative, less trade distorting, policy available to the local government, while under the GATS the outcome will depend on what GATS commitments have been made by the country, and only if so, would the question of a less trade distorting policy come to play.¹³²⁰

Aaronson had also correctly stated, based on an examination of six aspects shown in the graph below, that “cross-border data flows are quite different from trade in goods or other types of services. In sum, cross-border data flows moving across borders may not fit the traditional definition of trade.”¹³²¹

¹³¹⁴ WTO. *General Agreement on Tariffs and Trade 1994*, https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm, (1994). (“GATT”).

¹³¹⁵ WTO. *General Agreement on Trade in Services*, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm, (1995). (“GATS”).

¹³¹⁶ WTO. *Agreement on Trade-Related Aspects of Intellectual Property Rights*, https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm, (15 April 1994). (“TRIPS”).

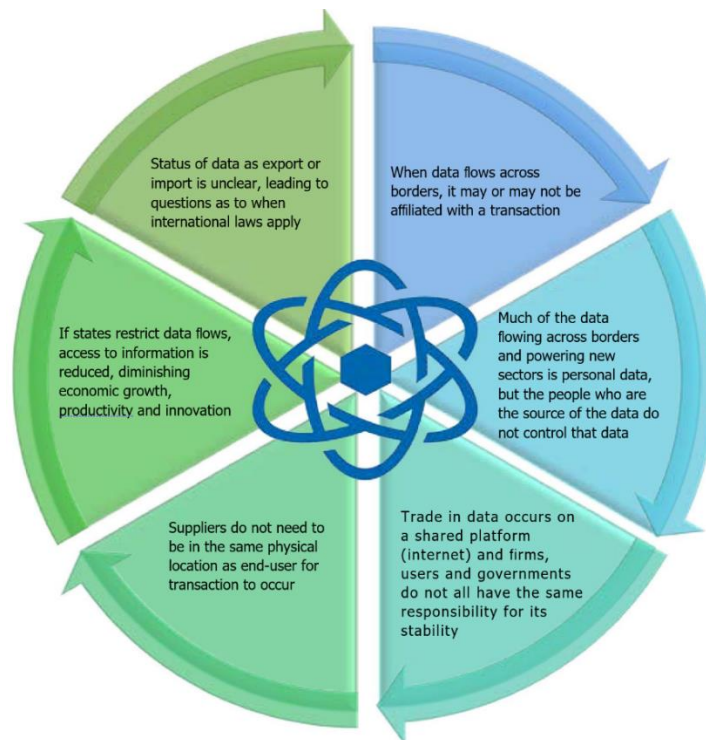
¹³¹⁷ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 147.

¹³¹⁸ WTO. *Services sectoral classification list*, MTN.GNS/W/120, (10 July 1991). P. 2

¹³¹⁹ The special feature of a national treatment obligation is that it does not arise directly from the conclusion of the GATS agreement but requires bilateral negotiations in which the WTO members individually agree on which opening clauses are to be entered into regarding individual service sectors. These “commitments” are then included in a WTO-held publicly available list.

¹³²⁰ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 28–29.

¹³²¹ Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 4.



Source: Aaronson, S.A. [Susan Ariel], "Cross-border Data Flows Are Different from Trade in Goods or Other Types of Services"¹³²²

Nevertheless, the European Communities and their Member States found that "Computer and related services, regardless of whether they are delivered via a network, including the Internet, include all services that provide [...] data processing, data storage, data hosting or database services"¹³²³. Crosby noted that "the transfer of data is necessarily included within the definition and scope of the data base services sector because these services must operate together in order for the data base services to be supplied at all"¹³²⁴. For the purpose of this thesis, a TFPD is therefore deemed to fall below Art. I(2)(a) GATS

Art. I(2) GATS defines "trade in services" as the supply of a service: "(1) from the territory of one Member into the territory of any other Member". The WTO refers to this as "Mode 1 — Cross border trade"¹³²⁵. In addition, Art. XXVIII(b) GATS defines the "supply of a service" as including "the production, distribution, marketing, sale and delivery of a service". However, it may be questionable whether TFPD fall under this Mode 1. In a dispute settlement on US Gambling Services, the WTO panel report confirmed that

mode 1 under the GATS encompasses all possible means of supplying services from the territory of one WTO Member into the territory of another WTO Member. Therefore, a market access commitment for mode 1 implies the right for other Members' suppliers to supply a service through all means of delivery, whether by mail, telephone, Internet

¹³²² Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 5.

¹³²³ WTO. *Communication from the European Communities and their Member States. Coverage of CPC 84 – Computer and Related Services*, TN/S/W/6S/CSC/W/35, (24 October 2002). P. 2.

¹³²⁴ Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, *International Centre for Trade and Sustainable Development (ICTSD)*. <https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 6.

¹³²⁵ WTO. (2022). *1.3 Definition of Services Trade and Modes of Supply*. https://www.wto.org/english/tratop_e/serv_e/cbt_course_e/c1s3p1_e.htm.

etc., unless otherwise specified in a Member's Schedule. We note that this is in line with the principle of technological neutrality, which seems to be largely shared among WTO Members.¹³²⁶

Moreover, GATS is recognized to be a "living agreement under which the scope and meaning of commitments evolve to accommodate technological advances, specifically concerning new forms of service delivery, but also covering digital services that fall within the coverage of existing commitments."¹³²⁷ We agree therefore with Crosby, who found that "Mode 1 trade in services includes the cross-border flow of data as required to produce, distribute, market, sell and deliver services internationally"¹³²⁸ and that the application of "Mode 1 does not require the supplier's presence or operation in a foreign country"¹³²⁹.

All members of the WTO are Parties to GATS. States wishing to join the WTO must submit to GATS. In addition, a dispute settlement procedure has been agreed, which applies to disputes between Member States concerning rights and obligations under the WTO agreements. The principle of a free TFPD, connected with the freedom of information, can constitute a restraint on State measures which are designed to restrict the export or import of personal data. Limiting fundamental rights in national constitutional law can endanger possible obligations of a State towards its undersigned international agreements. These obligations may arise from GATS. A regulation of TFPD can therefore clash with obligations stemming from GATS for WTO Member States.

GATS contains the fundamental prohibition of overt and covert discrimination by WTO members against other WTO members. Non-discrimination stems from two core principles of GATS, which are the so-called "MFN treatment"¹³³⁰ and the so-called "national treatment"¹³³¹. A discrimination can arise by putting the same services on a better or worse footing without any objective reason, which would contradict the goal of liberal trade. A discriminatory measure taken by the Member State can be covered by a justification and if it is necessary for the achievement of the regulatory objective.

Both GATT and GATS include "general exception" clauses. Art. XX in GATT allows Member States to take measures that are "necessary to protect public morals", while Art. XXI of GATT allows members to take "any action which it considers necessary for the protection of its essential security interests". Art. XIV of GATS allows Member States to take measures that are "necessary to protect public morals or to maintain public order", and measures needed for the "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts". Thus, both GATS and GATT provide for the national

¹³²⁶ WTO. *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Panel*, WT/DS285/R, (10 November 2004). P. 202.

¹³²⁷ Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, International Centre for Trade and Sustainable Development (ICTSD)*. <https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 4.

¹³²⁸ Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, International Centre for Trade and Sustainable Development (ICTSD)*. <https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 2.

¹³²⁹ Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, International Centre for Trade and Sustainable Development (ICTSD)*. <https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 3.

¹³³⁰ "Most-favored-nation treatment" (MFN treatment) (Art. II GATS) means that a State must grant the treatment it grants to one trading partner, whether or not that partner is a party to the agreement, to all other trading partners to the agreement.

¹³³¹ "National treatment" (Art. XVII GATS) means that legal or natural persons from the territory of one member, when acting in the territory of another member, may not be discriminated in comparison with domestic competitors.

security exception, while GATS also includes the “public order” exception. These exceptions are independent from each other and are not necessarily linked. However,

two major reasons justify a parallel assessment of the two exceptions hereinafter: (i) The most important services issues in the globalized world concern cross-border data flows in practice; public moral/order and security are highly relevant in this content. (ii) Politics in real life show that nation states usually invoke public moral/order and/or security reasons if services trade restrictions jeopardize the cross-border data flow.¹³³²

Such measures must not be applied “in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on trade in services”, Art XX GATT. To apply these exceptions, a “necessity test” is required, Art. XX GATT, Art. XIV GATS. A so-called “dispute settlements panel” decides whether another measure was available. According to Geist¹³³³, the necessity test contains the following four requirements: “it must achieve a legitimate public policy objective; it cannot be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination; it cannot be a disguised restriction on trade; and it must not impose restrictions greater than required to achieve the objective (i.e., a minimal impairment requirement on the use or location of computing facilities)”. These requirements could be applied to measures restricting TFPD. This will be subject to Chapter VIII, Section I.

¹³³² Baisch, R. [Rainer] and Weber, R. [Rolf]. (2018). Revisiting the Public Moral/Order and the Security Exceptions under the GATS. *Asian Journal of WTO & International Health Law and Policy*, 13(2), 375–394. P. 377.

¹³³³ Geist, M. [Michael]. (4 April 2018). *Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. A CIGI Essay Series on Data Governance in the Digital Age.* https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security/?utm_source=twitter&utm_medium=social&utm_campaign=data-series.

CHAPTER VI: SELF-REGULATION

At this point of the thesis, the question of a practical alternative or at least supplement to binding global data protection rules has to be raised. One approach could be to address the problems mentioned by a problem-oriented integration of stakeholders in the global ecosystem of TFPD¹³³⁴ when developing data protection rules. Private sector stakeholders could also be involved in corresponding regulatory activities. In the following, the approaches of self-regulatory efforts in the field of data protection are examined to outline whether and when they could contribute to an international regulation of TFPD.

State regulation, which is carried out solely by a State, is the most interventionist option¹³³⁵. This regulatory type is primarily done through legal rules imposed unilaterally and without the participation of private actors. The most intense participation of private actors lies in “pure self-regulation”. Compared to State regulation, pure self-regulation stands at the opposite end of the scale of the possible participation intensity of a State. Pure self-regulation is carried out solely by private actors without State participation. Based on the assumption that State participation within self-regulation is conceivable in addition to purely State regulation, there are graded stages depending on the degree of State participation in self-regulation. Two intermediate stages between pure State regulation and pure self-regulation can be identified as different levels of cooperation between the State and private individuals: “regulated self-regulation” and “co-regulation”. Regulated self-regulation results in a division of regulatory tasks between the State and private actors. It provides the State with a legal framework that can be used voluntarily by the private sector and, if necessary, be completed in such a way that the private sector can specify and further develop the requirements. With this form of self-regulation, the law has the function of granting powers, while the reservation of approval by the State is upheld. The law can support self-regulation for example through arbitration procedures or supervision of possible cases of abuse. This type of self-regulation is found in SDPC, BCR and CBPR, but also in CoC and certification.

Co-regulation is characterized by the fact that regulation is negotiated directly between State and private actors. State and private actors jointly set up rules by contributing to the development of the rules, for example in the context of negotiations, working groups and common institutions. In contrast to regulated self-regulation, co-regulation places a different emphasis on the cooperation between the State and the private sector. A State will continue to be involved in regulating, while the private sector can also influence the content itself.

¹³³⁴ See Chapter IX, Section I.

¹³³⁵ As to the options for an intervention to be analyzed in Chapter XI.

I. Pure self-regulation

This type of regulation is based on voluntariness, which means that there is no corresponding legal obligation for self-regulation. It can substitute State regulation or – as to be examined in Chapter VI Section II – step alongside State regulation.

Within the scope of pure self-regulation, a distinction can be made between explicit self-regulation and implicit or spontaneous self-regulation. Explicit self-regulation applies to cases if private sector stakeholders agree on certain rules of conduct and take a corresponding decision to comply with them. Implicit self-regulation can take place outside the organization, e.g., controlled by the market; or within the organization, e.g., promoted by a corresponding corporate culture. Since such implicit self-regulation provisions are not expressly stipulated by nature, the extent of this type of self-regulation can hardly be determined due to a lack of insight into the organization's workflows.

1. Guidelines

One way to establish certain rules of conduct is to use quality management as an organizational measure for a company which leads to an explicit in-house self-regulation. Quality management tries to match the performance of the company with the expectations of customers and to work towards products that meet customer requirements. Customer expectations also include that their data are adequately protected; that is why the quality management of a company must achieve a corresponding practice in all data processing and thus prevent data breaches that could go public and damage the reputation of the company. Since quality management in many companies is independent of State borders, the results for the level of data protection in the company concerned apply largely internationally. However, more detailed information on the respective quality management measures in individual companies is usually not available to outsiders.

Since the processes in a company are assessed based on certain criteria, at least in the case of an external audit process, the respective data protection measures are exceptionally comprehensible from the outside. The criteria for successfully completing an audit process are regularly known to the public. Only if these are met a corresponding audit seal be issued. The level of data protection achieved would nevertheless be company dependent. The benefit of quality management for an – at least to a certain extent – uniform global level of data protection is therefore low.

Many companies have also published privacy policies on their websites as self-binding regulations. These are data protection declarations in which the companies explain their data protection measures so that they are visible to data subjects. There is no globally recognized legal obligation for companies to develop privacy policies; they are voluntary. In some States, however, privacy policies can also be used to comply with legal information requirements. The privacy policies usually explain how and for what purpose personal data are collected, processed and forwarded by the company. The quality of the privacy policies varies between the individual companies. While some privacy policies are limited to short, very general information, others provide more detailed information.

Privacy policies define a certain type of data protection and are basically suitable for minimizing the information gap between companies and data subjects. Privacy policies are often drawn up very laboriously and are difficult to understand for the average reader. As a result, data subjects often refrain from reading those policies. It is therefore

repeatedly emphasized that data protection declarations that are too long and complicated do not correspond to the interests of the data subjects and that rather short and understandable data protection declarations are required. This applies in particular to the part of the data protection declaration that relates to consent. Correspondingly, the EDPB updated its guidelines on consent on 5 May 2020.¹³³⁶ The published guideline can be seen as an effort to bring clarity to the design of cookie banners and to put a stop to circumventions of GDPR requirements.

Privacy policies are often used across State borders for the entire group of companies and can therefore also apply in States where there are no statutory data protection requirements. If there is a *de facto* approximation of those policies of different affiliates, privacy policies can offer a useful approach to harmonize data protection across companies and regardless of State borders, since they can also be used to define a certain level of data protection in countries without data protection laws.

The OECD made a program available on the Internet that companies could use to develop or revise their privacy policy.¹³³⁷ This so-called “Privacy Statement Generator” automatically creates an individual privacy policy based on the answers of the companies to a series of questions about their current data protection practice. Unfortunately, after more than 10 years of use, the Privacy Statement Generator had to be discontinued due to technical overhauls.¹³³⁸

Data protection seals, which private bodies issue to interested companies when observing certain data protection requirements, could also be an option within a guidelines approach. These seals of approval are published on a company’s website and inform the consumer that there is a certain level of data protection. That way, the consumer should be encouraged to use the services of this company. The best-known quality seal provider is currently the US company TRUSTe LLC (TRUSTe). Other prominent examples are the “Trust Guard Privacy Verified Program”, “eTrust” and “Webtrust”. TRUSTe awards its data protection seal of approval to companies that comply with certain data protection requirements and agree to participate in their own dispute resolution procedure that their customers can use. TRUSTe must also be granted access to TRUSTe’s customers online areas and, upon request, relevant information on data processing activities to facilitate a compliance check against data protection rules. Customers of the verified companies can also make complaints to TRUSTe. Data protection seals of approval can, at least to a limited extent, standardize the level of data protection across States if the requirements of the seal of approval providers develop into a general standard on a global level. This presupposes that more companies make use of seals of approval and thus achieve a greater distribution. Companies could primarily choose to use data protection seals if they can use them for advertising purposes. The basic marketing value of such seals is higher than that of privacy policies, since seals reveal a particular data protection practice at a glance. However, it is currently not foreseeable that user trust will be oriented towards such seals of approval to a much greater extent in the future and that these will subsequently become more widespread.

There are efforts by the business community to create explicit self-regulatory provisions outside the organization, for example in the form of common rules of conduct developed

¹³³⁶ EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*,

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, (4 May 2020).

¹³³⁷ OECD. (24 July 2006). *Making Privacy Notices Simple: An OECD Report and Recommendations*, *OECD digital economy Papers*, No. 120. OECD Publishing. <https://doi.org/10.1787/231428216052>.

¹³³⁸ OECD. (2022). *OECD Privacy Statement Generator*.

<https://www.oecd.org/Internet/ieconomy/oecdprivacystatementgenerator.htm>.

independently of government regulations. In the area of TFPD, the “Global Network Initiative” (GNI)¹³³⁹ and recommendations of the “International Chamber of Commerce” (ICC) should be mentioned as examples. The GNI, with members such as Google, Microsoft, and Meta, develops rules for dealing with government requests for information and protecting freedom of expression, but less for personal data processing. The ICC developed various voluntary codes of conduct that help companies set standards for best practice. The ICC is intended to strengthen self-regulation of the economy and prevent government intervention. For some current issues, task forces are used as working groups for a limited time under the umbrella of certain commissions.¹³⁴⁰

Supported by this task force, the ICC published a “Privacy Toolkit”¹³⁴¹ in 2004 to show governments innovative ways of data protection regulation. The toolkit contains basic data protection principles based on the OECD Guidelines 1980 and makes suggestions for their implementation, based on instruments such as rules of conduct, contractual clauses or seals. The toolkit does not recommend restrictive data protection regulations. So far, however, the ICC has largely restricted itself to influencing governments with reference to corporate interests. The development of global data protection standards by the ICC would only be conceivable if it would create comprehensive guidelines for behavior in the area of data protection, which are also aimed at companies. Given the previous emphasis on corporate interests by the ICC in its data protection activities, it would be of importance whether and to what extent the protection of data subjects is also given importance.

2. Privacy Enhancing Technologies

It could be also conceivable to further develop Privacy Enhancing Technologies (PET). The OECD defines data protection through technology as digital systems that try to reduce the risks to data protection by using or incorporating goods and services.¹³⁴² The World Wide Web Consortium (W3C) could also play a role, as the guidelines developed for the Internet are of worldwide importance. The W3C had set up a “Tracking Protection Working Group”. However, data protection through technology without State funding has so far only been used to a limited extent. The efforts of the developers and manufacturers of technical products will primarily be directed at increasing customer satisfaction and trust. The advantages of data protection through technology are still too small to outweigh the costs of data protection through technology being used extensively. The previous approaches to data protection by technology also do not represent a comprehensive data protection concept, but only building blocks that cover certain areas such as anonymization or pseudonymization. Comprehensive data protection for all conceivable situations can hardly be achieved with technology alone. Data protection through technology initially requires the existence of certain data protection requirements, compliance with which is ensured by the technical precautions. However, this approach could form an assistance since only automated protective measures with a view to the hardly manageable global data flows can provide extensive data protection and data security.

¹³³⁹ Global Network Initiative. (2022). *About*. <https://globalnetworkinitiative.org>.

¹³⁴⁰ E.g., see USA, Federal Communications Commission. (2023). *Privacy and Data Protection Task Force*. <https://www.fcc.gov/privacy-and-data-protection-task-force>.

¹³⁴¹ ICC. (November 2033). *Privacy toolkit. An international business guide for policymakers*. <https://iccwbo.org/content/uploads/sites/3/2004/08/ICC-Privacy-Toolkit.pdf>.

¹³⁴² OECD. (2022). *Privacy Online: OECD Guidance on Policy and Practice”, Part III, Inventory of Privacy-enhancing Technologies (PETs)*.

<https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/reg%282001%291/final>.

II. Co-regulation

Existing approaches to co-regulation in data protection are located primarily at the international level. In supranational law, such as in the relationship between the EU and its Member States, there are numerous “opening clauses”¹³⁴³. Soft law is also important in a number of institutions, such as the ICC, the “International Organization of Securities Commissions” (IOSCO), the “United Nations Educational, Scientific and Cultural Organization” (UNESCO), the “International Institute for the Unification of Private Law” (UNIDROIT), the “United Nations Commission on International Trade Law” (UNCITRAL) and UNCTAD. Nonbinding soft law could be suitable for international co-regulation in the field of data protection. Soft law exists in the form of normative resolutions, declarations of intent, for example in the context of final reports on summits or international conferences, guidelines or recommendations from institutions that monitor compliance with contracts, as well as codes of conduct. Negotiations by the States with sometimes very different data protection concepts often result in an agreement on the lowest common denominator. With non-binding regulation, on the other hand, it could be easier than within the framework of a binding international agreement to reach a consensus since there is the possibility of deviating behavior and there is no threat for a loss of sovereignty. Furthermore, advocates of this approach (especially in business and government) suggest that it allows a much greater degree of flexibility than “traditional” regulation.¹³⁴⁴ Classic contracts that are binding under international law are often too cumbersome, since changing them is often time-consuming. If soft law would be developed through co-regulation, the advantages of self-regulation could be used. The knowledge of the non-State actors could be integrated and an increased willingness to comply with the regulations could then be assumed. Since States are also involved in the development of the requirements, the disadvantages of pure self-regulation could be reduced at the same time. Nevertheless, there are also downsides of such co-regulation. “On the other hand, critics (who often seek to protect consumer or citizen interests) believe that it is symptomatic of a wider trend towards the abdication of public matters to private self-interested actors, with consequent problems of democratic legitimacy”.¹³⁴⁵ Struggling enforcement mechanisms and sanctions are other downsides.

1. Guidelines

At the international level, the OECD, among others, developed a system in which certain regulations are developed in the form of recommendations in cooperation with companies. Dialogue with large international companies was sought when the OECD Guidelines were being developed in 1980. There is also close cooperation with private actors in the “Working Party on Information Security and Privacy” (WPISP), which was renamed in December 2013 as the “Working Party on Security and Privacy in the digital economy” (WPSPDE). The background to the existence of the WPSPDE is that the specialist work of the OECD takes place in the committees and working groups, of which there are around 200 (among others, the “Committee for Information, Computers and Communications Policy” (ICCP)). WPSPDE reports to the ICCP, which in turn reports to the OECD Council. However, the work of the WPSPDE has so far not been able to lead to uniform global data protection.

¹³⁴³ These allow the EU Member States to deviate in certain areas from the GDPR.

¹³⁴⁴ Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US 'Safe Harbor' Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield. P. 101.

¹³⁴⁵ Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US 'Safe Harbor' Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield. P. 101–102.

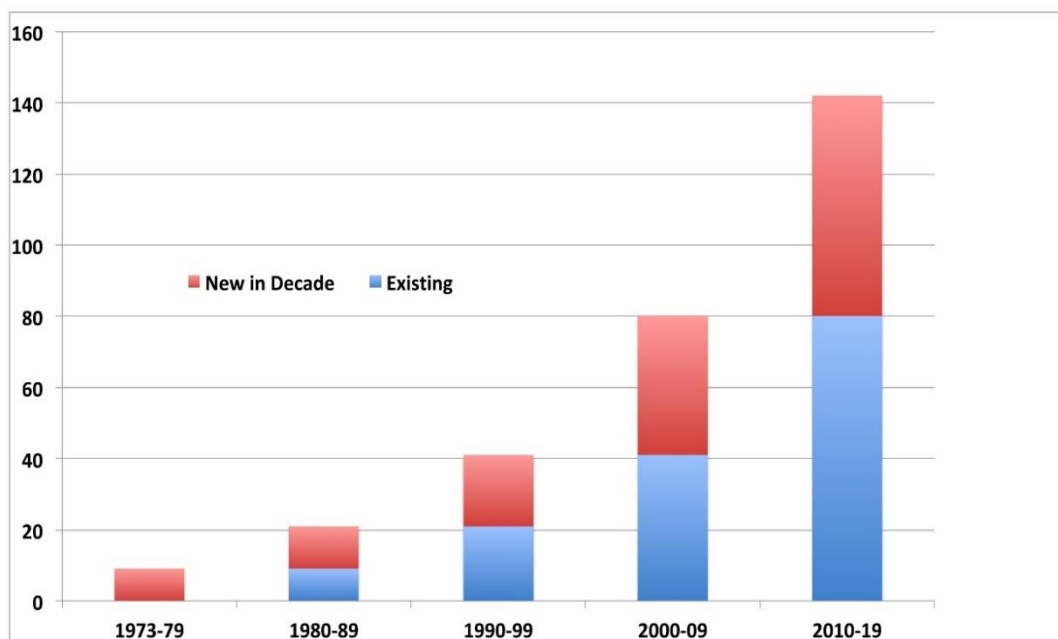
2. Privacy Enhancing Technologies

Cooperation between public and private bodies within the framework of the ISO could also be of practical importance in this respect. These standards stipulate a certain management procedure to guarantee a high level of data security and represent ultimately guidelines for behavior. The inclusion of private individuals in the development of standards in turn favors that they are also used in practice. In addition, there are specific technical standards for some technical questions that also concern data protection. In principle, the ISO already has the necessary structures in place for creating international requirements through co-regulation. The ISO standards in data protection primarily create guidelines for management systems. Certain goals and measures are defined, which, among other things, should ensure adequate protection through appropriate precautions of the system. These standards relating to management are to be assigned to the rules of conduct already discussed. On the other hand, there are – besides ISO 27701 developed to provide a standard for data privacy controls, which, when coupled with an “Information Security Management System” (ISMS), allows an organization to demonstrate effective privacy data management – hardly any specifications for data protection technology in the ISO standards discussed so far and are mostly not very specific. However, the ISO has also issued standards that contain, for example, specifications for cryptography and thus ultimately serve data security and data minimization principles. Nevertheless, the potential of the ISO for global data protection has already been recognized. At 26th Conference of Representatives for the Protection of Privacy and Data Protection in Wroclaw 2004, the recommendation was made to develop international standards and especially international technical standards for data protection through the ISO.¹³⁴⁶ Although ISO followed this recommendation by elaborating some standards, it does not intend to create a legislative framework with the existing standards such as ISO / IEC 27799. The current standards of ISO only contain detailed information for individual technical questions and thus firm guidelines for practical use. If standards theoretically affect an entire group and its systems, ISO normally avoids detailed specifications to enable them to be used as widely as possible.

¹³⁴⁶ ICDPPC. (14 September 2004). *Resolution on a Draft ISO Privacy Framework Standard*. <https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-a-Draft-ISO-Privacy-Framework-Standard.pdf>.

CHAPTER VII: CONCLUSIVE REMARKS ON THE REGULATORY MOSAIC

Since 1973, nations around the world have enacted data protection laws at an average rate of three new national laws per year, giving a total of 142 laws by December 2019, and probably over 200 by end-2023.

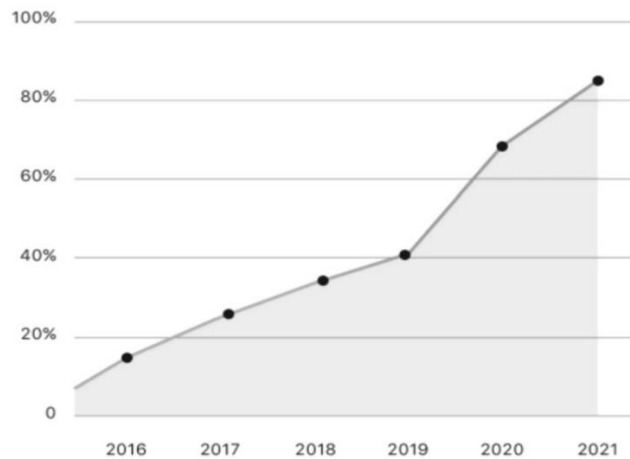


142 countries with data privacy laws by December 2019

Source: Greenleaf, G. [Graham] and Cottier, B. [Bertil], "2020 Ends a Decade of 62 New Data Privacy Laws"¹³⁴⁷

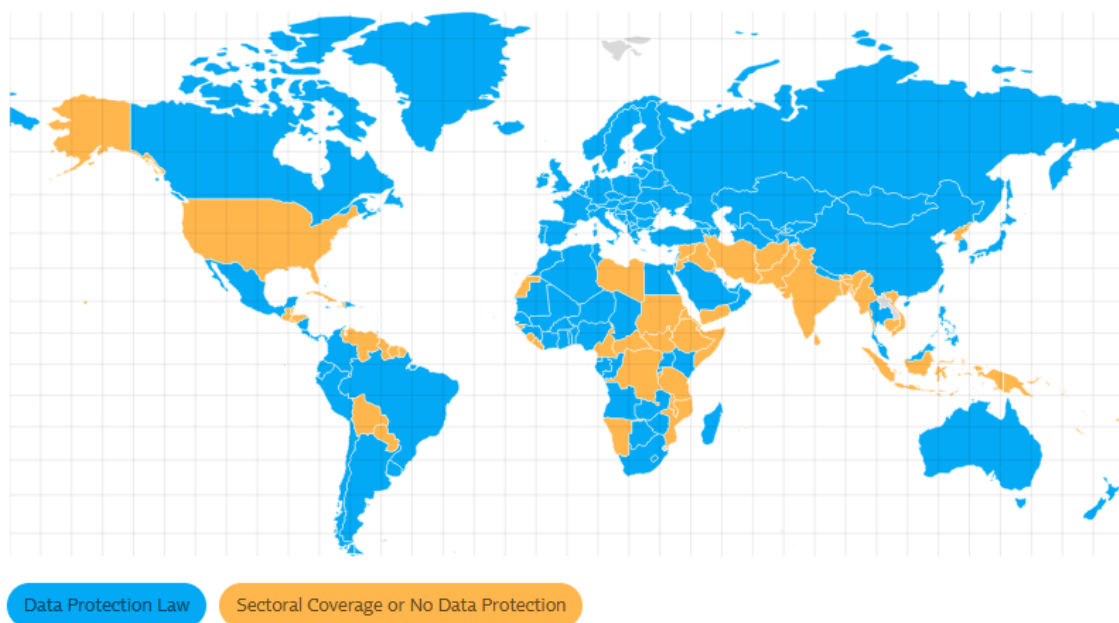
This made the proportion of individuals worldwide who are protected by modern data protection law increase to 83%.

¹³⁴⁷ Greenleaf, G. [Graham] and Cottier, B. [Bertil]. (2020). 2020 Ends a Decade of 62 New Data Privacy Laws. *Privacy Laws & Business International Report*, Vol. 163, 24–26. P. 24.



Source: Ethyca, "Percentage of world's population protected by a modern privacy law"¹³⁴⁸

To protect those individuals, there is a mosaic of regulations at international, supranational, and national level, which – explicitly or implicitly, legally binding, or non-binding, by unilateral, bilateral or multilateral, geographically-based or organizational-based rules – are concerned with the TFPD. Many nations have already comprehensive data protection legislation in place, others have such in some sectors, though others have no data protection regulations at all. The coverage of data protection laws differs, sometimes widely, as Chapters II-VI explained and the following graphic underlines.



Source: IAPP, "Global Privacy Law and DPA Directory"¹³⁴⁹

The Internet as technological function fundamentally questions national regulations. Data protection as a legal area is subject to a rapid change due to technical developments. Traditional regulation by a State alone can no longer guarantee an adequate level of protection. A State can often only react to technical developments and is slowed down by overlapping and increasingly inconsistent laws. As data processing

¹³⁴⁸ Ethyca Inc. (2023). *About*. <https://ethyca.com/about>.

¹³⁴⁹ International Association of Privacy Professionals. (June 2023). *Global Privacy Law and DPA Directory*. <https://iapp.org/resources/global-privacy-directory>.

by private and governmental actors is expanding day by day, aspects of data protection have become a focus of national and international law. The analyzed legal frameworks tried to react to this development. Nevertheless, the considerable differences between them, the lack of relevant, effective data protection regulations in practice at the global level and the associated different national data protection systems affect challenges, and ultimately also various approaches by policy makers.

There is a need to respond to the globality of the Internet with new regulatory concepts. In this regard, we fully agree with two appropriate findings in the literature. The first is by Trakman / Walters / Zeller, who stated that

Regulation, no matter the jurisdiction, to date, has been selective, fragmented and far from universally adopted. A related consequence is that data subjects did not receive direct rights of action against data users who allegedly misused their personal data. The result [...] is a smorgasbord of seemingly incompatible methods of using, protecting and regulating that data. Therefore, a purposive study is needed to determine the perceived extent to which personal data can be used and abused; the nature, source and extent of that abuse; the means currently employed to redress that abuse; the success of those means to date; and the prospects of adopting effective and fair measures to address deficiencies in those regulatory measures. [...] The resulting regulatory framework is also reductionist as states seek to develop their domestic laws, including data protection laws, to meet localized needs and public policy. The end-product is the marginalization of transnational public policy, such as the modes of data protection that are ideally shared across state boundaries, rather than subordinated to divergent state laws. As highlighted earlier this is further complicated by the fact that sovereign states view privacy over the Internet differently, even though a shift has commenced and there is a general acceptance of privacy over the Internet.¹³⁵⁰

We agree also with Weber / Staiger, who found that

many variables play a role in effectively regulating privacy in the digital world. These variables include embracing technology and its ability to increase the efficiency of our daily lives. Innovation and technological development cannot be stopped, thus legal scholars are tasked with identifying what legal concepts are still applicable to the digital age and disregard others that must be replaced by new and more appropriate concepts. This is highly challenging, as the existing legal norms are based on century-old principles and notions such as property which do not easily translate into the digital era and often come into conflict with other laws such as data protection. Thus, further research on an international level is necessary in order to develop new approaches to these issues which present an opportunity at harmonizing laws at a very high level with regard to new technologies, such as IoT, Big Data, and artificial intelligence (AI).¹³⁵¹

¹³⁵⁰ Trakman, L. [Leon] and Walters, R. [Robert] and Zeller, B. [Bruno]. (2019). Is Privacy and Personal Data Set to Become the New Intellectual Property?. *International Review of Intellectual Property and Competition Law*, 937–970, <http://dx.doi.org/10.2139/ssrn.3448959>. P. 964–965.

¹³⁵¹ Weber, R. [Rolf] and Staiger, D. [Dominic]. (2017). *Transatlantic Data Protection in Practice*. Springer. P. 137.

SECOND PART: THE PATH TO OVERCOME THE REGULATORY MOSAIC

The SECOND PART starts with an analysis of the problems (Chapter VIII) of the non-harmonized regulatory mosaic on TFPD (a mosaic presented in the FIRST PART). To eliminate those problems, there are three sides to consider. On the one hand a regulatory one, on the other hand a cooperative one, and lastly an economic one. The regulatory side is the traditional toolkit to manage problems through permission reservations. The cooperative side means that the addressing of problems is not the sole task of a State and should not be consistently enforced by it against the economy. Lastly, the economic side comes into consideration to influence market behavior in a self-regulating way through agreements and other economic instruments.

Including all stakeholders in a blended governance framework might encompass all these sides. To achieve this, a legislator needs a good preparation regarding all influencing dimensions. The following points are relevant in this respect: (i) knowledge of the facts, i.e., all the facts a legislator wants to influence or change (FIRST PART); (ii) analysis of the causes together with an overarching problem statement (Chapter VIII), as well as (iii) objectives (Chapter X) and (iv) options (Chapter XI) of an intervention. Chapter IX deals with stakeholders interests, and its location may not be obvious in the systematics of this thesis. It could have been located right before the details of the regulatory intervention to be proposed. However, we assume that the knowledge of a possible “common ground” within the matter of TFPD regulation becomes important even before certain regulatory objectives are worked out, because those objectives should not be aimed at those which would be absurd based on the interests elaborated in Chapter IX. Also, the location of stakeholder interests in Chapter IX, immediately before analyzing objectives of an intervention in Chapter X, is more in line with the above-mentioned EU policy and law-making cycle. Chapter XII should then answer the last research question, namely, which regulatory content an intervention should include and how the preferred intervention should be operationalized.

CHAPTER VIII: PROBLEM CATEGORIES AND PROBLEM DRIVERS

To determine the possibility of a regulatory intervention, regardless of the legal framework in which it can be carried out, it may be useful to consider the steps by the Commission in making such interventions. The “Intervention Logic”¹³⁵² concerns the question of whether, and, if so, how, a regulatory intervention can be carried out. The Commission divides this logic into five steps, which correspond to specific Chapters of this thesis, as outlined in the following table.

European Commission’s Intervention Logic:	1) Problem	2) Problem drivers	3) General objective	4) Specific objectives	5) Options			
					Non-legislative		Legislative	
					A	B	C	D
Chapters of this thesis:	Chapter VIII		Chapter X		Chapter XI			

The present Chapter VIII is the start of all parts of the Intervention Logic and the next step within the “specific methodology” of this thesis. As far as possible, all problems that might motivate a legislator as a “problem impulse”¹³⁵³ to undertake a normative activity should be covered. Chapter IX does not appear in the table above. The reason for this must be shown by first delimiting the objectives of Chapters VIII and IX.

We recognize the inherent risk of the structure of this thesis, that an appropriate “problem definition” can possibly only take place when stakeholder interests are already identified based on a public consultation phase of a regulatory intervention. However, the focus of Chapter IX will not be on stakeholder assessments which condense problem definitions but will rather lie on an analysis of stakeholder interests important for a future-oriented consensus regarding a possible regulation ahead. It is important to keep in mind this finer target direction of “stakeholder interests” – in contrast to the “Intervention Logic” – when reading Chapters VIII and IX.

At this point, “problem categories” and “problem drivers” must be distinguished and related to the four “dimensions” mentioned above¹³⁵⁴. “Problem drivers” lead to certain “problems”, which in turn lead to “consequences” that can be assigned to specific categories. The “core problem” usually binds all “problems” and “consequences” together. In the example of the “framework for the free flow of non-personal data in the European Union”, the “core problem” was the “obstacles to data mobility in the EU single market”¹³⁵⁵.

¹³⁵² See above Chapter I, Section II.4.

¹³⁵³ Noll, P. [Peter]. (1973). *Gesetzgebungslehre*. Rowohlt. P. 72f.

¹³⁵⁴ Chapter I, Section I.

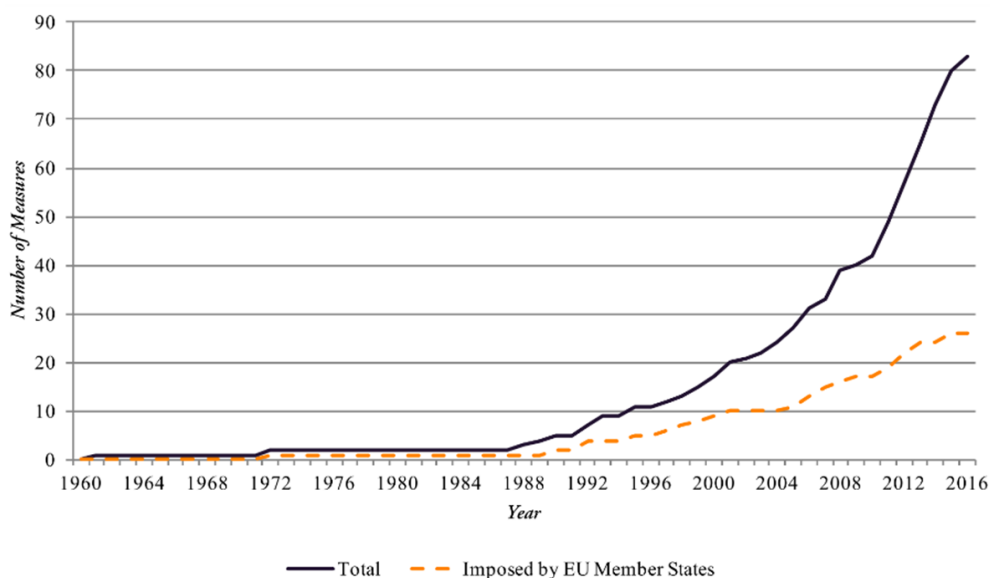
¹³⁵⁵ European Commission. *Commission Staff Working Document. Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, SWD(2017) 304 final*, (13 September 2017). P. 4.

I. The dilemma of a free flow of data vs. data flow restrictions

All regulatory instruments examined in Chapters II–VII aim at a free flow of data (including personal data). This gives reason to believe that the foremost assumption could be to qualify restrictions on flows of data (including personal data) as undesirable if adequate safeguards are in place. However, an UNCTAD report found that researchers

survey only adverse effects of data regulation. While this would be correct based on economic theory, with the underlying assumption that the market leads to efficient outcomes, it neglects the presence of market imperfections – such as monopolistic tendencies or societal values – that might generate other outcomes. From a more technical perspective, the assumptions underlying general equilibrium models and their calibrations may limit the generalizability of the findings to different country samples. [...] [Hereby] oversimplifications in the policy debate in the form of calls for free data flows across the board (or bans on data localization) on one extreme, and outright data localization as a general rule on the other extreme, are unlikely to be of much use. It is necessary to assess deeply what the implications of cross-border data flows are, taking into account differences among countries, types of data, interests and policy objectives.¹³⁵⁶

It is therefore necessary to examine in more detail – as the first focus of this Chapter VIII – the extent to which the tension between a free TFPD and restrictions of TFPD constitutes a “core problem”.



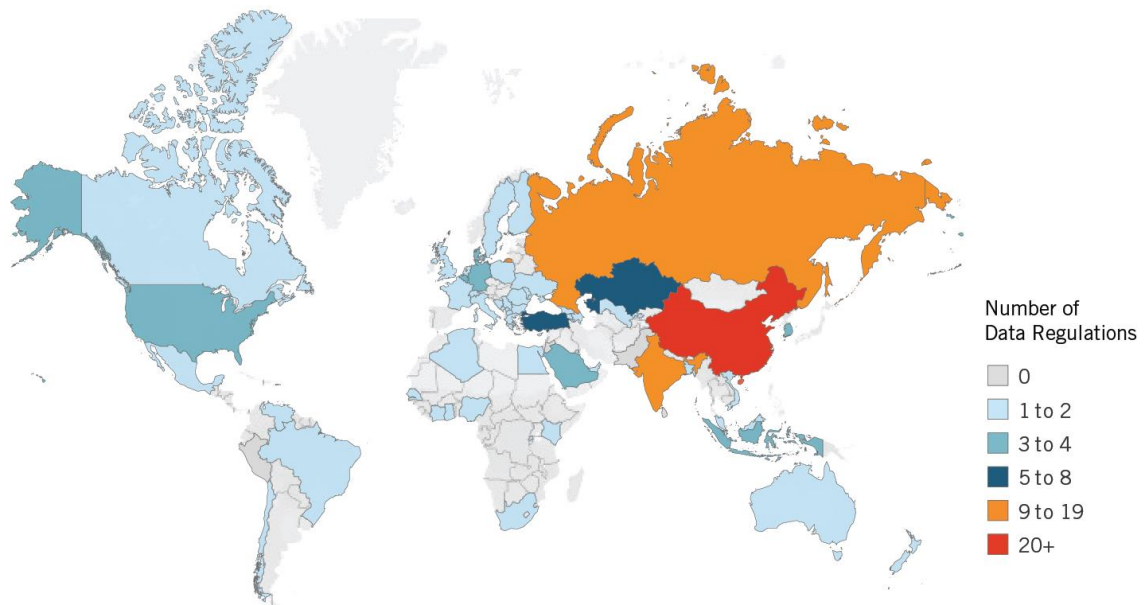
Source: ECIPE, “Number of data localization measures implemented globally and intra-European Union”¹³⁵⁷

As the graphic above shows, there is a trend towards more restrictions to transfers of personal data over the last five decades. Data, including personal data, will flow transborder unless governments enact restrictions. Governments faced an increasing reliance on such data in their economies, which “raised concerns among policymakers

¹³⁵⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 60, 93.

¹³⁵⁷ Bauer, M. [Matthias] and Ferracane, M. [Martina] and Lee-Makiyama, H. [Hosuk] and van der Marel, E. [Erik]. (December 2016). *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localization Measures in the EU Member States*. <https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu>. P. 4.

that felt the need to respond promptly to this development with new legislation”¹³⁵⁸. A study found that the “number of countries that have enacted data localization requirements has nearly doubled from 35 in 2017 to 62 in 2021. The number of data localization policies (both explicit and *de facto*) has more than doubled from 67 in 2017 to 144 in 2021. [...] China (29), India (12), Russia (9), and Turkey (7) are world leaders in requiring forced data localization.”¹³⁵⁹ The following graphic illustrates the distribution of these data localization policies.



Source: Information Technology & Innovation Foundation, “Blocking the global flow of data”¹³⁶⁰

This may have effects on the “right to information”, being it the freedom to transfer and receive information, commonly recognized by international human rights treaty bodies. First formulated in the UDHR, it is also provided in the ICCPR and in all supranational human rights conventions at regional level. Similar applies to the right to data protection, which, e.g., the ECHR protects in its Art. 8. In 2016, the UN Human Rights Council released a non-binding resolution condemning intentional disruption of internet access by governments as a human rights violation and an addition was made to Art. 19 of the UDHR (The Right to Internet Access).¹³⁶¹ Nevertheless, neither the right to information nor the right to data protection are unlimited. Limitations may be prescribed to protect public values.

These limitations are an “increasingly common way for a nation to assert data sovereignty, particularly if the country is not in a dominant position of geopolitical power [...]. Generally, governments want to claim sovereignty over their citizens’ data no matter where or by whom it is stored”¹³⁶². This “data sovereignty”, or sometimes also called “cybersovereignty” or “digital sovereignty”, which can be defined as “control over data

¹³⁵⁸ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

¹³⁵⁹ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

¹³⁶⁰ Information Technology & Innovation Foundation. (2021). *Blocking the global flow of data*. <https://cdn.sanity.io/files/03hnmfjy/production/451f8f1ffc72e97686f6bad3244706e7b8b7c6b.png>.

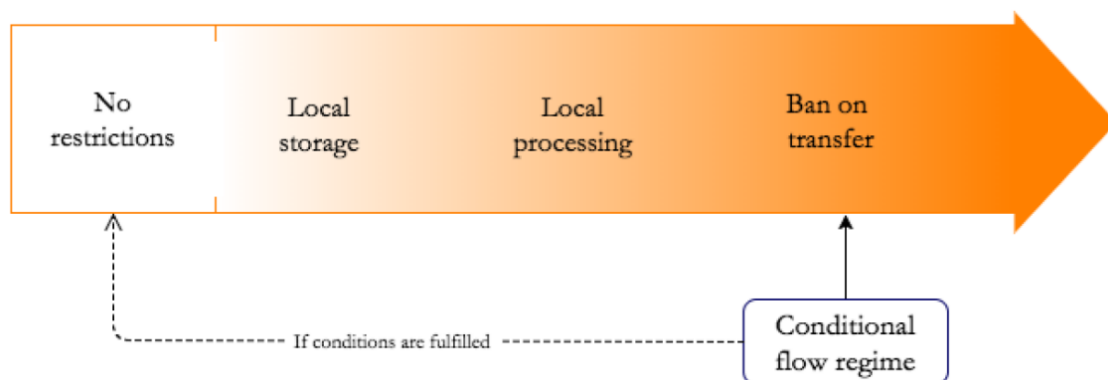
¹³⁶¹ United Nations, General Assembly. *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/32/L.20, (27 June 2016).

¹³⁶² Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 5.

through assertions of geopolitical power, international agreements about sovereignty recognition, and domestic policy creation”¹³⁶³, is therefore an overarching category of data flow restrictions.

Achieving the primary goal of governments “to curb foreign governments’ access rights to data stored outside of their jurisdiction”¹³⁶⁴ is pursued through an increasing variety of measures to restrict flows of personal data. These measures can be divided by their restrictiveness, which considers, on the one hand, the types of data involved, and on the other hand whether they are “strict” or “conditional” measures. Some governments restrict a TFPD only for data types such as health data and financial data. Others defined vague categories involving “important,” “critical” or “core” data.¹³⁶⁵ Third, “*de facto* data flow restriction” is also growing.

The strictest type is the obligation that data created within State borders must stay within those borders, which can encompass: “I: Local storage requirement; II: Local storage and processing requirement; III: Ban on data transfer (i.e. local storage, local processing and local access requirement).”¹³⁶⁶ A so-called “conditional flow regime” “can result in a system in which data can flow freely when the conditions are fulfilled, or in a ban on the transfer of data when the conditions are not fulfilled”¹³⁶⁷ and can encompass: “I: Conditional flow regime where conditions apply to the recipient country; II: Conditional flow regime where conditions apply to the data controller or data processor.”¹³⁶⁸



Source: Ferracane, M. [Martina], “Restrictions to Cross-Border Data Flows: a Taxonomy”¹³⁶⁹

¹³⁶³ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 5. // “Protectionism remains a key motivation behind many countries enacting data localization practices, but it has been subsumed into a broader narrative around cybersovereignty (also called data sovereignty or digital sovereignty) and control.” See Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>. // “Europe’s ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies).” See European Parliament. (July 2020). *Digital sovereignty for Europe*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf). P. 1.

¹³⁶⁴ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 3.

¹³⁶⁵ See Chapter VIII, Section I.2.

¹³⁶⁶ Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>.

¹³⁶⁷ Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>.

¹³⁶⁸ Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>.

¹³⁶⁹ Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>.

As these types of data flow restrictions ranging from the least restrictive to the most restrictive specify at least parts of a framework archetype as such, they will be discussed in more detail below¹³⁷⁰.

The question is how this “new form of protectionism in the era of AI and Big Data, or digital protectionism”¹³⁷¹ is justified by the legislators. The rationales can be “misguided data privacy and cybersecurity concerns [...], but cybersovereignty and censorship are newer, and in many ways, more-troubling motivations given they are broader and more ideologically driven.”¹³⁷² Rationales for introducing those restrictions typically include one or more of the rationales of “national digital economy / economic development lens”, “national security / public order / sovereignty lens”, and “adequacy and gaps in coverage / citizens” protection policy lens”.¹³⁷³ Each of these rationales, if not justified, then implies a problem driver described in Sections I.1. through I.3.

Interests in maintaining economic development have the most in common with security interests, and a certain security policy may ultimately serve to obscure the interests in an economic policy. Eduardo Ustaran also noted in this respect that

data localization first became noticeable as a tool of political control. Authoritarian regimes saw it as an extension of their core government policies. It provided easier access to information about any digital activities taking place within a country’s border while limiting the ability to disseminate information outside that border. [...] In recent times however, the motivation behind data localization has been primarily economic. In other words, data localization has become a powerful tool in support of economic protectionist policies. This trend has affected both autocratic and democratic countries as globalization as a concept became somewhat tainted.¹³⁷⁴

Data localization as a tool of political control is, however, as often overlooked in literature today, not exclusively a 21st century phenomenon. As early as 1984, Russell Pipe found that

trends can be found in a 1977 U.S. Government report on international service industries. It mentions that there is a growing tendency in many countries to require that data files remain in the country of origin rather than be transmitted across national boundaries. This conclusion received little attention at the time, but just two years later a State Department policy statement on international communications contained this sentence: The United States has national security, political, ideological, economic and technological stakes in international communications. A formidable challenge in the 1980s is how to reconcile the traditional principle of an open and largely unrestricted flow of information across borders with legitimate protective measures and outright protectionism.¹³⁷⁵

¹³⁷⁰ Chapter IX, Section III.1.4.1.

¹³⁷¹ Tomiura, E. [Eiichi] and Ito, B. [Banri] and Kang, B. [Byeongwoo]. (14 March 2020). *Cross-border data transfers under new regulations: Findings from a survey of Japanese firms*. <https://voxeu.org/article/cross-border-data-transfers-under-new-regulations>.

¹³⁷² Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

¹³⁷³ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 120.

¹³⁷⁴ Ustaran, E. [Eduardo]. (16 June 2022). *In search of a data localization strategy*. <https://www.linkedin.com/pulse/search-data-localization-strategy-eduardo-ustaran>.

¹³⁷⁵ Pipe, R. [Russell]. (1984). International information policy: Evolution of transborder data flow issues. *Telematics*, 1(4), 409–418. P. 414–415.

With the increase in digital services and goods, regulatory stakeholders are more confronted with this problem thirty years later. As an abstract example, data from a national company could be transferred to national servers, while a foreign company with a seat within this nation's territory transfers data abroad for data processing for the same type of value chain. A restriction on TFPD would then render the foreign company's service/product less competitive while a ban on such transfers would effectively prohibit the foreign company's service/product unless it undertakes related data processing (including storage) locally. These restrictions then "bear upon conditions of competition between foreign and national suppliers".¹³⁷⁶ The so-called "AI nationalism" can serve as a concrete example related to a particular technology. The Chinese government had announced its intention to achieve global dominance in AI by 2030.¹³⁷⁷ This subsequently led to a conflict between the US and China, escalating with the Committee on Foreign Investments in the US tightening the conditions for foreign companies to invest in American tech companies.¹³⁷⁸ On Chinese side, Art. 37 CSL is used for the same tightening conditions by requiring certain types of data to be stored within China and security approvals if transferring these data abroad. Hogarth therefore believed that States slow down or even prohibit foreign investment and acquisitions of AI startups, intensify relations with national companies, and set standards and regulations internationally in a way that benefits the national industry.¹³⁷⁹

Since the US exercises data sovereignty from a strong position due to its geopolitical power, it tended to be less focused on applying restrictions in general, and in particular for the protection of the national digital economy, although this approach started to change during the Trump administration. The US noted in the course of the WTO Work Program on Electronic Commerce that

all Members share an interest in the protection of privacy and the security of data. [...] Nonetheless, Members must ensure that, in the spirit of promoting trade, such measures are subject to appropriate discipline. In the view of the United States, there is little evidence to support the need for restricting data from being exported to a particular country's territory solely because the destination country does not share a formal privacy or data security regime with the source country. [...] Members as such must take great care that any measures that prevent data exports or that mandate local storage must not constitute an unjustified barrier to trade, unduly discriminating against the foreign supply of any information-intensive service, including but not limited to data processing.¹³⁸⁰

Other States, such as Russia or China, which apply more measures to restrict TFPD, scatter them across different rationales.

1. National digital economy

As noted above¹³⁸¹, TFPD can lead to economic and social benefits. The use of information and communication technologies is a "key element of infrastructure for efficient industries and a critical productivity enhancer [which] is crucial for sustaining

¹³⁷⁶ OECD. *Trade and cross-border data flows*. TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 29.

¹³⁷⁷ Mozur, P. [Paul]. (20 July 2017). Beijing Wants A.I. to Be Made in China by 2030. *The New York Times*. <https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html>.

¹³⁷⁸ Rappeport, A. [Alan]. (17 September 2019). U.S. Outlines Plans to Scrutinize Chinese and Other Foreign Investment. *The New York Times*. <https://www.nytimes.com/2019/09/17/us/politics/china-foreign-investment-cfius.html>.

¹³⁷⁹ Hogarth, I. [Ian]. (13 June 2018). AI Nationalism. *Ian Hogarth*. <https://www.ianhogarth.com/blog/2018/6/13/ai-nationalism>.

¹³⁸⁰ WTO. *Work Programme on Electronic Commerce - Communication from the United States*, S/C/W/359, (17 December 2014). P. 3-4

¹³⁸¹ Chapter I, Section I.2.; and Chapter I, Section I.3.

recovery and laying the foundations for economies that are competitive in the long term”¹³⁸² and “will remain crucial not only for developed countries for sustaining and enhancing their innovation potential and long-term competitiveness, but also for middle-income and developing countries in fostering structural transformations, increasing efficiency as well as reducing the digital, economic, and social divides within their territories and vis-à-vis more advanced economies”¹³⁸³. The main drivers for these benefits are globally acting MNEs. Therefore, from an economic perspective, “the outsourcing of data processing can often make sense; however, the implications of outsourcing for privacy must be examined, particularly if the data protection laws of the countries concerned are not in harmony”¹³⁸⁴. These “implications” are increasingly being considered in the context of “national digital economy policies” to encourage in-country data processing. As there is a “presumed global consensus on trade – as evidenced by membership in the World Trade Organization – there should, at least in theory, be able to be a consensus on digital trade issues”¹³⁸⁵. However, there are gray areas between different rationales for the implementation of such digital economy-related policies. The ways to protect or stimulate a national digital economy are therefore worth examining in this Section I.1.

The OECD found that there is “no data on data” and that there is “a lack of data on the volume of cross-border data transfers” and it is therefore difficult to determine origin and destination because data flows in mysterious ways; furthermore, “data is different (it is valued by its utility, not by its volume, is not scarce, can be copied and shared virtually for free)”; finally, it is “difficult to say how companies use and derive value from data” and “to measure the economic value of trust.”¹³⁸⁶ The tools to understand the economic impact range from “ex-ante models”, to “ex-post models, through “firm level surveys”, and “combinations of the above”.¹³⁸⁷

Tomiura, Ito and Kang noted that “it is practically impossible for an academic researcher to collect direct data on cross-border data transmissions by individual firms, especially in terms of economic values”¹³⁸⁸. Ferracane therefore correctly stated that “an accurate taxonomy of the restrictions on data flows is just one piece of the puzzle needed to answer this question. Further research is needed on two areas. The first is economic and relates to the impact of these measures on trade. It will be relevant to analyze how the costs of various restrictions or conditionalities vary, and how they affect business decisions of those entities engaged in international trade”¹³⁸⁹.

¹³⁸² Dutta, S. [Soumitra] and Mia, I. [Irene]. (2010). *Global Information Technology Report 2009–2010*. WEF. P. vii.

¹³⁸³ Dutta, S. [Soumitra] and Mia, I. [Irene]. (2010). *Global Information Technology Report 2009–2010*. WEF. P. v.

¹³⁸⁴ Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130. P. 118.

¹³⁸⁵ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 226.

¹³⁸⁶ Lopez Gonzalez, J. [Javier]. (9 November 2020). *Trade and cross-border data flows. Mapping the policy environment and thinking about the economic implications*. WTO Trade Dialogues. https://www.wto.org/english/res_e/reser_e/2_javier_lopez_gonzales_wto_dialogues_november_2020_rev3.pdf. P. 5.

¹³⁸⁷ Lopez Gonzalez, J. [Javier]. (9 November 2020). *Trade and cross-border data flows. Mapping the policy environment and thinking about the economic implications*. WTO Trade Dialogues. https://www.wto.org/english/res_e/reser_e/2_javier_lopez_gonzales_wto_dialogues_november_2020_rev3.pdf. P. 6.

¹³⁸⁸ Tomiura, E. [Eiichi] and Ito, B. [Banri] and Kang, B. [Byeongwoo]. (14 March 2020). *Cross-border data transfers under new regulations: Findings from a survey of Japanese firms*. <https://voxeu.org/article/cross-border-data-transfers-under-new-regulations>.

¹³⁸⁹ Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>. P. 6.

This task of producing a taxonomy was taken up in the summer of 2021 by Cory / Dascoli in an extensive study of 46 countries.¹³⁹⁰ Their model “calculates a composite index – the data restrictiveness linkage (DRL) – to estimate the linkage of downstream industries with national data restrictiveness (based on the data intensity of those industries)” and “is based on econometric best practices as demonstrated by OECD and European Center for International Political Economy (ECIPE)”.

Roßnagel noted that the DGA is “the first attempt to harmonize data use and data protection in normative terms. This is achieved primarily by the fact that the GDPR also retains its full validity in the area of the data economy and is supplemented by the Data Governance Act only selectively with regard to three types of controllers: public bodies, data intermediaries and data altruistic organizations. With regard to data protection, it makes sense to differentiate between personal and non-personal data”¹³⁹¹. It must therefore be remembered at this point that this thesis is limited to personal data.

Steinrötter recognized that the “demarcation problems between personal and non-personal data could cause legal uncertainty, in particular if the distinction is used to delineate legal fields from each other” and that there is a “problematic relationship between non-personal data, whose free sharing is seen as economically and publicly desirable, and personal data, whose use in the EU is subject to existing stringent rules (now found in the GDPR) aimed at protecting the data subject’s privacy”¹³⁹², although a free flow of personal data is, besides the protection of fundamental rights, still an objective, but under certain safeguards. Since techniques to measure implications mostly involve “mixed datasets” (both personal and non-personal data), the question therefore becomes more difficult as to whether restrictions in favor of a national digital economy policy are demonstrably a “problem driver” for the purposes of this thesis.

As an example, intra-EU data flow restrictions should be mentioned here. An ECIPE study¹³⁹³ identified 22 of such measures “where European Union Member States impose restrictions on the transfer of data to another Member State. The most common restrictions target company records, accounting data, banking, telecommunications, gambling and government data. In addition, there are at least 35 restrictions on data usage that could indirectly localize data within a certain Member State”. It is noticeable that these restrictions are mostly in the finance sector. The study went on to note that such measures “create a major misallocation of resources and threaten the continent’s productivity and competitiveness” and therefore recommended adding “a ban on unjustified restrictions on the location of data for storage or processing purposes” to the EU’s Digital Single Market Strategy. Goldfarb and Treffer argued that “data localization is a privacy policy that could favor domestic firms”¹³⁹⁴. However, this is countered by other opinions.

The Commission recognized that the

¹³⁹⁰ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

¹³⁹¹ Roßnagel, A. [Alexander]. (2021). Grundrechtsschutz in der Datenwirtschaft. *Zeitschrift für Rechtspolitik*, 54(6), 173–176. P. 175.

¹³⁹² Steinrötter, B. [Björn]. (2020). Legal Framework for Commercialization of Digital Data. In M. [Martin] Ebers and S. [Susana] Navas (eds.), *Algorithms and Law* (pp. 269–298). Cambridge University Press. P. 273.

¹³⁹³ Bauer, M. [Matthias] and Ferracane, M. [Martina] and Lee-Makiyama, H. [Hosuk] and van der Marel, E. [Erik]. (December 2016). *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localization Measures in the EU Member States*. <https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu>. P. 1.

¹³⁹⁴ Goldfarb, A. [Avi] and Treffer, D. [Daniel]. (2019). Artificial intelligence and international trade. In A. [Ajay] Agrawal and J. [Joshua] Gans and A. [Avi] Goldfarb (eds.), *The Economics of Artificial Intelligence* (pp. 463–492). University of Chicago Press. P. 486.

data services market is substantially influenced by lack of transparent rules and a strong perception of the need to localize data. This may limit the access of businesses and public sector organizations to cheaper or more innovative data services, or force businesses operating cross-border to arrange excess data storage and processing capabilities. This could also inhibit data-driven businesses, in particular start-ups and SMEs, from scaling-up their activities, entering new markets [...] or centralizing data and analytics capacities in order to develop new products and services.¹³⁹⁵

The OECD found that

local storage requirements for data may have the effect of diverting trade and production to national suppliers of intermediate goods and services much like local content requirements [...]. While firms located in the domestic territory and engaged in the provision of data solutions may see their business activity increase as a result of the rise in local demand after the introduction of the measures, these gains are likely to accrue to a small segment of the firm population. Efficiency losses may arise in other firms from imposing domestic sourcing where foreign sourcing may be more cost-effective [...]. In this sense, a local storage requirement becomes analogous to a traditional import substitution strategy. Firms may also need to switch to potentially less reliable, less efficient and pricier local suppliers rather than accessing global digital services or international outsourcing solutions. Firms might also have to relocate or replicate certain functions, such as after-sales services or data management facilities, to particular countries in response to the measures. This will disrupt centralized business solutions which could lead to inefficiencies arising from the loss of access to scale opportunities [...]. It could further decrease the use and efficiency of trends like 'big data' and affect the development of new ICT industries.¹³⁹⁶

Tomiura, Ito and Kang analyzed which type of companies are most likely to be affected by regulations surrounding the TFPD. On the one hand, the study depicted that the share of firms affected by the regulations imposed by China and other emerging countries is nearly twice as high as the share affected by the GDPR. However, the study also showcased that companies' exposure to regulation increases when companies collect data overseas. 30% of the firms that reported impacts of the regulations have therefore "changed the location of data storage and/or data processing in response to regulations by EU and emerging countries, indicating a non-negligible impact on the geography of data-related activities"¹³⁹⁷, whilst many of these data flows are intra-firm. The study also highlighted

that the firms' responses to regulations vary substantially. More than 40% of the respondents have tightened data protection to meet the EU's requirement in response to GDPR. In contrast, more than half of the surveyed firms have not taken any measures against the cyber security regulations of China and other emerging countries, despite their recognition of the impacts of these regulations. Their inaction could possibly be due to the uncertainty associated with new regulations based on the lack of transparency in the rules created by these emerging countries.¹³⁹⁸

¹³⁹⁵ European Commission. *Building a European Data Economy*, COM(2017) 9 final, (10 January 2017). P. 6.

¹³⁹⁶ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Paras. 73–74.

¹³⁹⁷ Tomiura, E. [Eiichi] and Ito, B. [Banri] and Kang, B. [Byeongwoo]. (14 March 2020). *Cross-border data transfers under new regulations: Findings from a survey of Japanese firms*. <https://voxeu.org/article/cross-border-data-transfers-under-new-regulations>.

¹³⁹⁸ Tomiura, E. [Eiichi] and Ito, B. [Banri] and Kang, B. [Byeongwoo]. (14 March 2020). *Cross-border data transfers under new regulations: Findings from a survey of Japanese firms*. <https://voxeu.org/article/cross-border-data-transfers-under-new-regulations>.

This, as these authors noted in another summary of their study, leads to implications for firm-level productivity and for globalization in the digital age:

Firms that collect data overseas are, on average, more productive than firms that do not regularly collect data overseas (or in Japan) by 14-18%. [...] Firms that are active in cross-border data transmissions tend not only to be productive, but also globalized. [...] Digital data are intensively transmitted across national borders by a limited number of large-sized, productive, and globalized firms. They are productive enough to cover non-negligible entry costs for cross-border activities, including data transfers across national borders. As the firms that are active in data transfers tend to be large, as well as active in many markets and able to trade with many partners, and possibly also exert wide spillover effects from their superior productivity, we should not underestimate the impact of regulations on cross-border data transfers.¹³⁹⁹

Emily Wu found that “local data storage does not necessarily mean improvements for the domestic economy [because data localization] raises the barriers for market entry, which suppresses entrepreneurial activity and reduces the ability for an economy to compete globally [and] in some cases, the cost of compliance is too great, leading large MNEs to exit a market which is ultimately detrimental to users”¹⁴⁰⁰. Another study noted that

requiring national data processing and storage or national digital service production restricts [business] activities to the relevant national scale of operation, and this is likely to lead to significantly higher costs of operation per customer served; Embeds other national production factors into digital services (e.g., if a country is subject to electricity supply constraints, these can be overcome in part through the use of international data storage and digital service production); Is likely to delay, limit or even prevent citizens’ access to innovative digital services that emerge on the global stage; and fails to acknowledge the value to the national economy of skills and insights that are only available if data can flow across borders.¹⁴⁰¹

We agree with those opinions that underline negative implications of restricting TFPD on a national digital economy, and see the opinion of Goldfarb and Treffer critical and too simplistic. Nevertheless, it must be acknowledged that a pure “data protection law”, including the use of data flow restrictions, may no longer serve the national interests of countries that are involved in the global digital economy.

Coming back to Ferracane, “the second [further research] area is legal, and relates to how the different restrictions in this taxonomy contribute to achieving the desired policy objective. In particular, it will be relevant to investigate certain policy objectives that fall under GATS exceptions in Art. XIV and XIV bis – such as data privacy, national security, prevention of (cyber) fraud and public order”¹⁴⁰².

In China, the data flow restrictions regime set by CSL, DSL and PIPL are in tension with China’s commitments under the WTO’s General Agreement on Trade in Services (GATS) and China’s recently stated desire to become a party to the Comprehensive and

¹³⁹⁹ Tomiura, E. [Eiichi] and Ito, B. [Banri] and Kang, B. [Byeongwoo]. (12 August 2020). *Regulating cross-border data flows: Firm-level analysis from Japan*. <https://voxeu.org/article/regulating-cross-border-data-flows>.

¹⁴⁰⁰ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 14–15.

¹⁴⁰¹ GSMA. (September 2018). *Cross-Border Data Flows Realizing benefits and removing barriers*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf. P. 16.

¹⁴⁰² Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>. P. 6.

Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the digital economy Partnership Agreement (DEPA), two Asia-Pacific regional trade agreements with strong disciplines on facilitating digital trade, including cross-border transfers of information.”¹⁴⁰³

In Europe, this tension with WTO rules urged the EDPB to issue a statement noting that “all international agreements involving the transfer of personal data to third countries or international organizations which were concluded by the EU Member States prior to 24 May 2016 or 6 May 2016 respectively, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked” and invited the Member States “to assess and, where necessary, review their international agreements that involve international transfers of personal data”.¹⁴⁰⁴ These agreements may also include horizontal provisions regulating data protection in trade agreements between the EU and third countries.¹⁴⁰⁵

Iakovleva summarized in this respect that “the risk that the EU’s commitment to liberalizing the cross-border movement of services under the General Agreement on Trade in Services (GATS), on the one hand, and to the protection of the fundamental right to the protection of personal data, on the other hand, will clash is very real”¹⁴⁰⁶. Similarly, Kulhari stressed that “in the context of data-driven trade, the EU data protection framework acts as an impediment to the cross-border transfer of data and can be said to have negative implications for free trade. In the event of a GATS based challenge to the EU data protection framework embodied in the GDPR, provisions restricting cross-border data transfer run significant risk of being rendered incompatible”.¹⁴⁰⁷ Naef also argued that

some aspects of the EU regulation of data transfers do not find justification under the privacy exception in Article XIV(c)(ii) GATS. This concerns due process requirements in cases in which a third country requests an adequacy decision according to Article 45 GDPR; special framework adequacy decisions for countries that otherwise would not qualify for a regular adequacy decision such as the invalidated Decision (EU) 2016/1250, the Privacy Shield adequacy decision for the US, or the planned adequacy decision for the Transatlantic Data Privacy Framework between the EU and the US; and inconsistencies in the use of the corrective powers to ban or suspend data transfers in Article 58(2)(f) and (j) GDPR by the supervisory authorities in the EU member states. Consequently, I found that the EU fundamental rights-based regulation of data transfers is compatible with WTO law as long as the due process requirements are complied with, no special framework adequacy decisions are adopted, and the supervisory authorities in the EU member states use their corrective powers actively and consistently to enforce the right to continuous protection of personal data.¹⁴⁰⁸

¹⁴⁰³ WilmerHale. (3 November 2021). *China Publishes Draft Measures on Security Assessment of Cross-Border Data Transfer*. <https://www.wilmerhale.com/en/insights/client-alerts/20201103-china-publishes-draft-measures-on-security-assessment-of-cross-border-data-transfer>.

¹⁴⁰⁴ EDPB. *Statement 04/2021 on international agreements including transfers*, https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf, (13 April 2021). P. 1.

¹⁴⁰⁵ See Chapter II, Section II.4.5.

¹⁴⁰⁶ Iakovleva, S. [Svetlana]. (2021). *Governing cross-border data flows: Reconciling EU data protection and international trade law*. [Doctoral thesis, Faculty of Law, Universiteit van Amsterdam (I. Venzke)]. <https://hdl.handle.net/11245.1/cf54d2a9-cd41-42c2-94f1-24c81f8a3abd>. P. 312.

¹⁴⁰⁷ Max Planck Institute for Innovation and Competition. (23 March 2021). *Global Convergence of Data Protection Norms: Agenda for Trade and Development*. <https://www.ip.mpg.de/en/projects/details/global-convergence-of-data-protection-norms-agenda-for-trade-and-development.html>.

¹⁴⁰⁸ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 425.

The potential conflict of new regulatory measures with obligations for WTO Member States is not only a phenomenon of the APAC framework or European framework. The OECD also addressed this and noted that

in the context of GATS, data localization measures require companies to take actions relating to how they handle the data that is necessary for the supply of a particular service. As such, localization measures will, in effect, relate to the supply of services as they bear upon conditions of competition between foreign and national suppliers. The data localization requirement could arguably create situations, not only *de jure* but also *de facto*, where foreign services and services suppliers are treated less favorably than domestic firms. However, the general exception clauses related to security, and public morals and privacy could negate the negotiated commitments from applying to data localization measures. For the public morals and privacy exception to be valid, the specific regulation needs to meet a necessity test, part of which is a requirement to respect the objectives of non-discrimination and least trade distorting alternatives to the regulation (GATS Article XIV).¹⁴⁰⁹

The next questions – consistent with WTO jurisprudence – are, firstly, whether treaty violations are established, and secondly, whether measures to restrict TFPD might be justified under the relevant exceptions; i.e., “General Exceptions” (Art. XIV GATS), “Security Exceptions” (Art. XIV bis GATS) or Para. 5(d) GATS Annex on Telecommunications. Regarding the nature of those exceptions.

At this point we must come back to the classification of TFPD under WTO law, because “the legality of a data localization policy might therefore turn on the sectoral classification of the affected product.”¹⁴¹⁰ It was found above¹⁴¹¹ that those transfers belong to GATS.

Whenever a service lies in a particular sector in which a Member has an obligation under GATS, it is – with Crosby – arguable that a “Member’s prohibition of even a single means of delivery through mode 1 will give rise to a violation, even if alternative means of non-remote or local delivery are allowed, or if supply is permitted through other means of delivery or modes of supply”¹⁴¹², as “the supply of such services necessarily requires the cross-border flow of customer and business data”¹⁴¹³. As explained above¹⁴¹⁴, TFPD have a significant impact on all sectors of the economy. It is therefore to be assumed for the further course of this thesis that restrictions of such flows affect the supply of services in all committed sectors and modes of supply. On the one hand, the “General Obligations and Disciplines” in Part II GATS, to which the above-mentioned¹⁴¹⁵ “MFN treatment” belongs, or even the “Specific Commitments” in Part III GATS, to which the above-mentioned¹⁴¹⁶ “national treatment” belongs, can be violated by data flow restrictions. The latter can in its most severe form also constitute an impermissible market access limitation under Art. XVI GATS. This depends on whether a restriction “totally prevents the use by service suppliers of one, several or all means of delivery that are included in

¹⁴⁰⁹ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Paras. 52–53.

¹⁴¹⁰ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Para. 49.

¹⁴¹¹ Chapter V, Section III.

¹⁴¹² Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, International Centre for Trade and Sustainable Development (ICTSD). <https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 3.

¹⁴¹³ Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, International Centre for Trade and Sustainable Development (ICTSD). <https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 3.

¹⁴¹⁴ Chapter I, Section I.2.

¹⁴¹⁵ Chapter V, Section III.

¹⁴¹⁶ Chapter V, Section III.

mode 1” ((falling then under Art. XVI(2)(a) GATS)) or the “limitation on the total number of service operations or on the total quantity of service output” ((falling then under Art. XVI(2)(c) GATS)).¹⁴¹⁷ In the context of the national treatment principle, the question would then be whether the data flow restriction measures lead to less favorable treatment to foreign suppliers of affected services. It has already been stated above that such measures increase costs of supplying services for foreign competitors. The national treatment principle, however, is not to be understood as an obligation for “formal” equal treatment under the law; rather, it can be sufficient if domestic as well as foreign suppliers are not provided with the same competitive conditions, i.e., no so-called “level playing field” is guaranteed.

Art. XIV(c)(ii) GATS could be relevant to justify favoring a domestic digital economy. Its aim is “the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.” A data flow restriction would also have to withstand a “two-tiered analysis”¹⁴¹⁸ developed in the above-mentioned “*US Gambling Services*” dispute settlement.¹⁴¹⁹ To this end, the first step would be to examine whether there is a causal relationship between the regulatory measure in question and its objective. The second step would be to examine whether the regulatory measure in question is the least trade restrictive. That is, whether there would be an alternative regulatory measure that would be less infringing of the GATS while providing the same level of data protection. This involves balancing whether the regulatory measure is more likely to make an indispensable contribution to data protection. The higher the general interest in data protection, the greater the contribution of the regulatory measure to the enforcement of the latter. The lower the degree of trade restriction, the more necessary the regulatory measure.

A detailed examination of the goal of protecting the national digital economy is beyond the scope of this thesis. We assume that such data flow restrictions would not be justified, because contractual access through multilateral and bilateral agreements would be a less infringing and similarly effective way to ensure regulators can perform their role to protect the national digital economy. In the case of access to personal data regulated by the US Cloud Act, for example, executive agreements that meet certain criteria as, e.g., the rule of law, can be concluded with other States. We therefore follow Crosby who stated that “where a WTO Member has scheduled commitments on the cross-border supply of data services, it will be very difficult for the Member to argue that data localization measures requiring foreign suppliers to duplicate infrastructure and services or to pay for outsourced local storage are consistent with GATS National Treatment rules”.¹⁴²⁰ Geist therefore also noted that “the historical record suggests that reliance on this exception is rarely accepted [...] as the GATT and GATS exceptions have only ever been successfully employed to actually defend a challenged measure in one of 40 attempts”, concluding that “the benefits of the general exception may be illusory since

¹⁴¹⁷ WTO. *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Panel*, WT/DS285/R, (10 November 2004). P. 215.

¹⁴¹⁸ “Specifically, that a measure must: (a) fall within the scope of one of the recognized exceptions set out in paragraphs (a) to (e) of Article XIV in order to enjoy provisional justification; and (b) meet the requirements of the introductory provisions of Article XIV, the so-called “chapeau”.”

¹⁴¹⁹ WTO. *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Panel*, WT/DS285/R, (10 November 2004). P. 235.

¹⁴²⁰ Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, International Centre for Trade and Sustainable Development (ICTSD)*.

<https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 8.

the requirements are so complex (each aspect must be met) that countries have rarely managed to meet the necessary conditions”¹⁴²¹.

The application of those exceptions was already a point of discussion at the time of the negotiations on the TiSA proposal¹⁴²². It was expressed that these clauses are considered the best protection against the loss of freedom of action in the area of data protection regulation.¹⁴²³ These clauses can allow WTO Members to continue to regulate their national data protection laws. However, certain conditions must be met so that national data protection laws cannot be considered a “barrier to trade”, warned the authors of a study, which examined the EU’s right to regulate transfers of personal data to third countries.¹⁴²⁴ The authors of that study “underscore the formula of the European Parliament that new free trade agreements better entrust their right to regulate in the field of privacy and data protection to a comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement, without any conditions that it must be consistent with other parts of the [agreement]”¹⁴²⁵. This study therefore argued that this right should also not be made dependent on qualitative conditions (e.g., “necessary”). This example shows that there are tendencies to make extensive use of exceptions such as Art. XIV GATS. Sacks therefore argued that

Beijing uses vague language in standards, like in many Chinese laws and regulations, to avoid issues, such as World Trade Organization (WTO) challenges, while allowing the government maximum flexibility and discretion to apply onerous provisions when it sees fit. Beijing must disclose required standards to the WTO. However, in 2017 the government downgraded over 1,000 Chinese standards submitted to the WTO from required national standards to recommendations.¹⁴²⁶

After 1997, “there has been no progress on improving the bound coverage of GATS commitments at the multilateral level. Countries have therefore attempted to make progress outside of the multilateral trading system in regional Free Trade Agreements (FTAs)”¹⁴²⁷. Past and current negotiations indicate that also future agreements are likely to include provisions on transborder data flows. One area of such negotiations is the regulation of intellectual property. Companies in different sectors depend on the proper protection of their intellectual property assets and want to enforce their rights at an international level, seeking means of enforcement that may impinge on individuals’ right

¹⁴²¹ Geist, M. [Michael]. (4 April 2018). *Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. A CIGI Essay Series on Data Governance in the Digital Age.* https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security/?utm_source=twitter&utm_medium=social&utm_campaign=data-series.

¹⁴²² The “Trade in Services Agreement” (TiSA), which included a commitment to free flow of data and a ban on data localization, was to be, from its design of the agreement, strongly oriented to the structures of GATS. It was a proposed international trade treaty between 23 Parties, including the EU, UK and the US. It has been put on hold in 2016, a specific end date for the negotiations is currently not foreseen.

¹⁴²³ Council of the EU. *Draft Directives for the negotiation of a plurilateral agreement on trade in services,* <https://data.consilium.europa.eu/doc/document/ST-6891-2013-ADD-1-DCL-1/en/pdf>, (10 March 2015). P. 4

¹⁴²⁴ Irion, K. [Kristina] and Yakovleva, S. [Svetlana] and Bartl, M. [Marija]. (13 July 2016). *Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements.* https://www.beuc.eu/publications/beuc-x-2016-070_trade_and_privacy-complicated_bedfellows_study.pdf. P. 46.

¹⁴²⁵ Irion, K. [Kristina] and Yakovleva, S. [Svetlana] and Bartl, M. [Marija]. (13 July 2016). *Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements.*

https://www.beuc.eu/publications/beuc-x-2016-070_trade_and_privacy-complicated_bedfellows_study.pdf. P. VIII.

¹⁴²⁶ Sacks, S. [Samm]. (7 March 2019). *Testimony on “China: Challenges to U.S. Commerce, A Hearing Before the Senate Committee on Commerce, Science, and Transportation’s, Subcommittee on Security.*

<https://www.commerce.senate.gov/services/files/7109ED0E-7D00-4DDC-998E-B99B2D19449A>. P. 3.

¹⁴²⁷ Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, International Centre for Trade and Sustainable Development (ICTSD).*

<https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 1.

to data protection. This results in an increasing danger for personal data, stressed by the problem of the existence of different levels of data protection in different jurisdictions, with regulators facing the challenge to balance the different interest at stake. Therefore, as the reach of the Internet expands, governments increasingly seek to introduce initiatives aimed at controlling individuals' online activity. One such initiative, aimed, inter alia, at introducing enhanced online copyright enforcement standards, was the "Anti-Counterfeiting Trade Agreement" (ACTA).¹⁴²⁸ ACTA was a planned multilateral trade agreement which provided for the establishment of an authority which obliges ISPs to disclose – at the request of a rights holder – the identity of data subjects who allegedly carried out an infringement using the ISPs' services. The competent authority did not necessarily have to be part of the judicial authorities. Neither there was a minimum threshold for the alleged legal infringement been specified, nor any requirements as to how the legitimacy of the request was to be proven. A vague suspicion might therefore be sufficient for the disclosure of the data subject. By vote of 4 July 2012 the European Parliament decided not to ratify ACTA. Other initiatives in the US, such as the "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act" (PIPA)¹⁴²⁹ and the "Stop Online Piracy Act" (SOPA)¹⁴³⁰ were also shelved. Like SOPA, PIPA was supposed to enable American copyright holders to prevent the unlawful distribution of their content on the Internet, including ways of so-called "DNS blocking". The "Intellectual Property Rights Enforcement Directive" (IPRED2)¹⁴³¹, the "Transatlantic Trade and Investment Partnership" (TTIP)¹⁴³², the "Canada-EU Comprehensive Economic and Trade Agreement" (CETA)¹⁴³³ and other initiatives show that the end of the ACTA proposal is far from being the end of the contents of ACTA, as their approach was similar.

2. National security and national public order

This Section 1.2 reviews whether the State interest of "national security / public order / sovereignty" are a rationale to justify data flow restrictions and whether this leads to the "core problem." The "World Economic Forum" (WEF) noted in this respect that

while some jurisdictions are open and make no distinction between foreign or domestic entities in their data protection rules, most jurisdictions make a distinction between domestic and foreign entities for data that is perceived to pertain to national security, or they designate specific entities as either trusted or of particular high risk – where some jurisdictions also routinely categorize all data as being sensitive.¹⁴³⁴

A study divided between "foreign surveillance", having as relevance that "internationally stored data may be vulnerable to surveillance by the foreign government or others", and "national security", having as relevance that "Internet platform companies and telecommunications operators that store data internationally may not be compelled to provide the same support to law enforcement or national security organizations".¹⁴³⁵

¹⁴²⁸ USA, Office of the United States Trade Representative. *Anti-Counterfeiting Trade Agreement (ACTA)*, <https://ustr.gov/acta>, (1 October 2011).

¹⁴²⁹ USA. *PROTECT IP Act of 2011*, S.968 (112th), (26 May 2011).

¹⁴³⁰ USA. *Stop Online Piracy Act*, H.R. 3261 (112th), (26 October 2011).

¹⁴³¹ European Commission. *Amended proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights*, COM(2006) 168 final, (24 June 2006). // The European Commission has withdrawn the IPRED2 proposal and thus terminated the IPRED2 Directive process.

¹⁴³² See Chapter II, Section II.4.3.

¹⁴³³ See Chapter II, Section II.4.3.

¹⁴³⁴ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 14.

¹⁴³⁵ GSMA. (September 2018). *Cross-Border Data Flows Realizing benefits and removing barriers*.

https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf. P. 10.

Since surveillance and national security are intertwined, we prefer to analyze both under “national security” in a broader sense. The rationale “public order” asserts the need to use the law to maintain order both in the legal and moral sense. This also includes measures of law enforcement, which are in turn also part of the exercise of sovereignty. Rationales for data flow restrictions are fluid and often referred to for various data categories falling below different derogations and exceptions, which allow a legislator to deviate from the principle of a free flow of personal data. These fluid boundaries can be illustrated by two examples:

The CoE noted that “the Convention does not restrict the freedom of a Party to limit the transfer of personal data to another Party for other purposes, including for instance national security, defense, public safety, or other important public interests (including protection of state secrecy)”¹⁴³⁶. The CoE stated further that “the notion of national security should be interpreted on the basis of the relevant case law of the European Court of Human Rights. The relevant case law includes in particular the protection of state security and constitutional democracy from, inter alia, espionage, terrorism, support for terrorism and separatism.”¹⁴³⁷ The notion usually includes “essential objectives of general public interest”¹⁴³⁸, which then needs to be checked for necessity¹⁴³⁹. Not only the CoE, which listed “the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security and public safety”¹⁴⁴⁰ as rationales, mentions these terms mostly in one sentence and in a way that blurs the differences of these terms.

Art. 5.6 of the Chinese PI Specification 2020, similar to the GDPR, mentions, for example, these data categories:

- Personal data directly related to national security or national defense;
- Personal data directly related to public security, public health or major public interests;
- Personal data directly related to criminal investigations, prosecutions, trials or execution of court decisions;
- Personal data for the purpose of safeguarding the life, property or other significant legitimate rights and interests of the PI Subjects or other individuals, and it is hard to obtain consent from the PI Subjects.

These fluid boundaries made it difficult for the Chinese legislator to make a demarcation between “core data”, “important data,” and “ordinary data”. “Important data” are closely related to national security, national economic development and public interest. “Core data” as a subset to “important data” are data that pose “a serious threat to China’s national and economic interests. Disruption of important data could cause major damage, leading to large-scale shutdowns, or large-scale network and service paralysis”¹⁴⁴¹. Art. 37 CSL regulates that OCII processing ordinary data or important data during operations within the Mainland China shall store such data within Mainland China.

¹⁴³⁶ Explanatory Report to Convention 108+. Para. 105.

¹⁴³⁷ Explanatory Report to Convention 108+. Para. 94.

¹⁴³⁸ Explanatory Report to Convention 108+. Para. 93.

¹⁴³⁹ See for example regarding Section 26 of UK’s Data Protection Act 2018: “The [national security exemption] applies if it is “required” to safeguard national security. In this context, “required” means that the use of the exemption is “reasonably necessary”. This is linked to human rights standards. This means that any interference with privacy rights should be necessary and proportionate in a democratic society to meet a pressing social need.” // See UK, Information Commissioners’ Office. (7 March 2022). *National security and defense*. <https://ico.org.uk/for-organizations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/#work>.

¹⁴⁴⁰ Explanatory Report to Convention 108+. Para. 92.

¹⁴⁴¹ Horwitz, J. [Josh]. (30 September 2021). China drafts new data measures, defines “core data”. *Reuters*. <https://www.reuters.com/world/china/china-issues-draft-rule-data-security-industry-telecoms-2021-09-30>.

Chinese law thus allows data flow restrictions for purposes of national security, to maintain public order or for reasons of the common good.

Data controllers with business in China must ensure not to “harm the rights and interests of the citizens of China or endanger China’s national security and public interests”, Art. 42 PIPL. China can take “corresponding measures [...] ‘where any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against China’ in relation to personal data”, Art. 43 PIPL. The latter is an important new step unknown to the European framework. It creates a new type of risk for companies, that rules they need to comply with in their own territory could lead to these companies becoming subject to Chinese “retaliatory actions”, which could make China an

increasingly difficult market for foreign firms to operate in. There are three main challenges posed by the standards regime: First, the Chinese government can use standards to pressure companies to undergo invasive product reviews where sensitive information and source code (even if not explicitly required) may be exposed as part of verification and testing. [...] Second, Chinese standards also create a competitive advantage for Chinese companies. [...] Third, to comply with some standards, foreign firms may need to redesign products for the China market where they are not compatible with international standards. [...] Restrictions on cross-border data flows represent one of the top problems for U.S. companies in China.¹⁴⁴²

The APEC Privacy Framework 2015, the ASEAN Framework on Personal Data Protection, the US Patriot Act, the US Cloud Act, the CCC, and the UN Guidelines, to name other examples at least briefly, also have rationales of “national security / public order / sovereignty” in a broader sense and partly exclude these matters from the scope of application of their data protection regulations. The UN Guidelines also include “morality” as possible exception in para. 6. Exemplarily, the US Patriot Act, is one of “large data collections based on legal sources which have been enacted with the ostensible objective of enhancing security to the benefit of all”¹⁴⁴³. Concerns about foreign surveillance of data stored in other national markets, however, were increasingly countered after the NSA affair with a

diversification of countries in which internet platform companies and cloud computing providers operate data centers or regional hubs. This allows organizations and governments that are concerned about foreign surveillance activities to avoid data being held in particular jurisdictions. However, allowing organizations this level of geographic control inevitably comes at a cost which must either be absorbed by the business customer or ultimately the downstream consumer.¹⁴⁴⁴

However, as Wu explained, extraterritorial scopes of application such as that of the Cloud Act can reduce the effectiveness of such “geographic control”.

The US Cloud Act has clarified that US tech companies are subject to US laws no matter where in the world they are operating, or whose data they are storing. This substantially reduces the efficacy of data localization laws as a mechanism to protect data stored by US companies from US law enforcement agencies because these

¹⁴⁴² Sacks, S. [Samm]. (7 March 2019). *Testimony on “China: Challenges to U.S. Commerce, A Hearing Before the Senate Committee on Commerce, Science, and Transportation’s, Subcommittee on Security*.

<https://www.commerce.senate.gov/services/files/7109ED0E-7D00-4DDC-998E-B99B2D19449A>. P. 2–4.

¹⁴⁴³ Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130. P. 118.

¹⁴⁴⁴ GSMA. (September 2018). *Cross-Border Data Flows Realizing benefits and removing barriers*.

https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf. P. 16.

companies remain within the jurisdiction of US law enforcement no matter where their servers may be located.¹⁴⁴⁵

In turn, organizations could counter this by encrypting data and keeping the keys nationally and resistant to decryption. Other techniques could be the anonymization of data. With these means, but at further cost, organizations could mitigate risks of foreign surveillance where data are held internationally.

In addition to *de facto* localization, the European framework also offers “several examples of pieces of existing legislation imposing to store personal data in the EU and that usually go even further by also restricting transfers”¹⁴⁴⁶. These include Art. 6(8)¹⁴⁴⁷ of the PNR Directive¹⁴⁴⁸, Art. 3 of the VIS Regulation¹⁴⁴⁹, Art. 41 of Regulation (EU) 2017/2226¹⁴⁵⁰, and Art. 39 of Regulation (EC) No 1987/2006¹⁴⁵¹, all related to an Entry/Exit System (EES), Schengen border control and law enforcement. The reach of protective elements in the European framework includes practically all aspects of social interaction online and has a stronger focus on the protection of personal data instead of other protected elements such as free speech. This might give rise to problematic effects such as creating obstacles to efficient law enforcement. The availability of services of today’s digital society leads to situations where infringements are conducted transborder. Jurisdictional limits can then act as “safe harbors” for the offenders. It is therefore “understandable that governments are concerned about losing access to data that may be useful to their law enforcement authorities, but which is processed and controlled by internet companies based outside of their countries”¹⁴⁵².

To solve this, enforcement bodies traditionally cooperated on transborder investigation of high-profile crimes. With the increase of such transborder cases it became inevitable for them to cooperate on daily-based investigation also of regular or minor offences. A need for a fluent exchange of information evolved. At the same time the challenge augmented to fulfill, e.g., investigative requests for evidence, in line with procedural requirements, so that principles of fair trial were not threatened. This applies in particular to so-called “e-discovery cases”. For the practice of international corporations, this legal discovery – originating from the Anglo-American area – is a frequent topic. The purpose of discovery is to store, collect and submit documents and other stored information for Parties in US trials. US corporations with subsidiaries e.g., in Germany, or German corporations with subsidiaries in the US can face e-discovery actions as plaintiff, as defendant or as a third party. The question of the justification of the data transfer then arises as a data protection implication. Art. 49(1)(e) GDPR allows data transfer from the

¹⁴⁴⁵ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 3–4.

¹⁴⁴⁶ EDPB. *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, (12 July 2022). Para. 106.

¹⁴⁴⁷ “The storage, processing and analysis of PNR data by the PIU shall be carried out exclusively within a secure location or locations within the territory of the Member States.”

¹⁴⁴⁸ See also Chapter II, Section II.3.6.

¹⁴⁴⁹ EU. *Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)*, OJ L 218, 60–81, (13 August 2008).

¹⁴⁵⁰ EU. *Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011*, OJ L 327, 20–82, (9 December 2017).

¹⁴⁵¹ EU. *Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, OJ L 381, 4–23, (28 December 2006).

¹⁴⁵² GSMA. (September 2018). *Cross-Border Data Flows Realizing benefits and removing barriers*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf. P. 16.

EEA to unsafe third countries, provided that “the transfer is necessary for the establishment, exercise or defense of legal claims”. Thus, another problem driver lies in the balance between the interests of data protection and judicial investigations.

The traditional principle of the jurisdiction to prescribe can eventually not solve problems of TFPD. A scenario could be criminal investigations carried out in State A, for which data that located on a server in State B are to be accessed. The authorities of State B would then have to be asked for support through legal assistance. The CCC also provides for this in Arts. 23, 25 and 31. However, it is questionable whether these forms of cooperation are fast and flexible enough to enable effective investigations. In the aforementioned¹⁴⁵³ distinction between types of jurisdictions, this would be assigned to a jurisdiction to enforce. In the non-virtual world, this would correspond to a search and seizure, if necessary, by investigators from a foreign State. With the conventional understanding of sovereignty and territoriality, this access would be impossible without consent. A corresponding access option could be contractually agreed. This problem was discussed in the negotiations on the CCC.¹⁴⁵⁴ However, only a partial compromise could be reached. Art. 32 of the CCC only regulates two largely unproblematic cases. According to Art. 32 of the CCC, access is permitted if the data are publicly accessible (lit. a) or if a person authorized to do so has consented to access (lit. b). One might think that this expresses that any other form of access should be excluded; however, this argument is explicitly excluded in the Explanatory Report.¹⁴⁵⁵

National laws based on the rationales discussed in this Section I.2 may also regulate the processing of personal data not only of their own citizens. This applies to the collection of intelligence, but also in the law enforcement area. This can then lead to countries preferring to draw a dividing line between citizens/persons residing in their own territory and all other persons. This possible discrimination was recognized with respect to the US after the NSA affair. Human rights organizations subsequently criticized the lack of data protection for non-US persons. The German and Brazilian governments had also submitted a joint resolution to the UN General Assembly calling attention to the human rights violations that can result from extraterritorial mass surveillance.¹⁴⁵⁶

Measures within the rationales of this Section I.2 have been critically addressed. Sacks recommended from a US perspective a “small yard, high fence” approach, which means

being selective about what technologies are vital to U.S. national security, but being aggressive in protecting them. Overreach in the form of blanket bans, unwinding global supply chains, and discrimination based on national origin is not the answer. Tools like the Committee on Foreign Investment in the United States (CFIUS), export controls, and law enforcement are designed to be used as scalpels, not blunt instruments.¹⁴⁵⁷

Such overreach can have negative effects. Regarding the “law enforcement” rationale, Weber noted that

apart from the inherent risks of such data collections, governments are put into a position where they have to deputize private sector organizations as law enforcement

¹⁴⁵³ Chapter I, Section II.5.6.

¹⁴⁵⁴ CoE. *Explanatory report to the Convention on Cybercrime*, (8 November 2001), Para. 293 f.

¹⁴⁵⁵ CoE. *Explanatory report to the Convention on Cybercrime*, (8 November 2001), Para. 293.

¹⁴⁵⁶ German Federal Foreign Office. (19 December 2013). *German Brazilian resolution on internet privacy adopted*. <https://www.auswaertiges-amt.de/en/aussenpolitik/internationale-organisationen/vereintenationen/131127-resolution-privatsphaere-im-internet/258450>.

¹⁴⁵⁷ Sacks, S. [Samm]. (7 March 2019). *Testimony on “China: Challenges to U.S. Commerce, A Hearing Before the Senate Committee on Commerce, Science, and Transportation’s, Subcommittee on Security*.

<https://www.commerce.senate.gov/services/files/7109ED0E-7D00-4DDC-998E-B99B2D19449A>. P. 6.

agents requiring them to transmit data and personal information that they have collected from individuals for entirely different reasons. Such requests have the function of a Trojan Horse for attacking private law privacy fortresses. The challenge is even increased if certain actions are merely done as fishing expeditions.¹⁴⁵⁸

Moreover, considerable doubts exist as to whether data flow restrictions actually lead to greater data security. Wu noted that “a smaller local provider may actually be at increased threat of security breach given their relatively smaller capabilities to protect against malicious actors”¹⁴⁵⁹. Similar comments were made by the World Economic Forum.

Experts universally agree data localization requirements have little positive impact on jobs or security since the productivity losses exceed the minuscule number of jobs created in data processing. Further, experts note that information security is not a function of where data are physically stored or processed geographically but rather how it is maintained. On the contrary, data localization requirements could lower companies’ ability to ensure cybersecurity or consumer protection, and could increase entry points for cyberattacks.¹⁴⁶⁰

Crosby also summarized that “many studies have demonstrated the security and reliability benefits of not storing all information in one place or jurisdiction.”¹⁴⁶¹ Another study noted that “ultimately, countries that turn their backs on services available in the global digital economy must fall back on national-scale production of goods and services. For their part, major commercial players in a national market will find it difficult to ensure a sustainable business if their operations are seen to undermine law enforcement or national security”¹⁴⁶².

Also within the national security rationale, a conflict may arise between WTO obligations of a Member State on the one hand and its data flow restrictions on the other hand. A violation of GATS rules could in turn be justified under Art. XIV GATS, as it explicitly mentions “measures that are necessary to protect public morals or to maintain public order” as a justification.

3. Adequacy and gaps in coverage

A *de facto* data flow restriction can happen in various ways, e.g., by requesting authorization prior to a transborder data transfer, by imposing high fines for violations of data protection rules, by requiring a different qualification of the legal nature of the right to data protection, or by stretching extraterritorial application of data protection rules. The aim of this Section I.3 is to present such rationales, which can all be grouped under the headline “adequacy and gaps in coverage”, respectively under the “citizens’ protection policy lens” in UNCTAD terms.

¹⁴⁵⁸ Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130. P. 118.

¹⁴⁵⁹ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 14.

¹⁴⁶⁰ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 9.

¹⁴⁶¹ Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, International Centre for Trade and Sustainable Development (ICTSD).

<https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>. P. 1.

¹⁴⁶² GSMA. (September 2018). *Cross-Border Data Flows Realizing benefits and removing barriers*.

https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf. P. 16.

A study found that responses to national privacy concerns begin with policymakers arguing “that personal data may not be protected when transferred internationally, and individuals may not have sufficient rights in countries that do not have the same safeguards. [...] This is arguably based on a misconception that data stored in a specific national market is more secure than data stored internationally.”¹⁴⁶³ The main rationales for policymakers that arise from such misconceptions are – with Kuner – preventing circumvention of national privacy and data protection laws, guarding against data processing risks in other countries, and difficulties in asserting data protection and privacy rights abroad.¹⁴⁶⁴ Ustaran found that “the existing restrictions of international data transfers have also contributed to this phenomenon, particularly in light of the increasing regulatory pressures to place controls on government access to data exported to other jurisdictions. Data localization has become a ready-made solution to what is often presented as an irresolvable conflict of laws”.¹⁴⁶⁵ Cory / Atkinson / Castro found that

policies that lead to local data storage can actually undermine personal data protection, as without an independent judiciary and set of legal protections, governments can bring more pressure and tools to bear in forcing local providers to disclose data (for both social and political purposes). Even if a data privacy framework only requires a copy of data to be stored locally, rather than prohibiting transfers of all data, it nevertheless lays the groundwork for such an outcome. Furthermore, wherever data privacy intersects with cybersecurity, forced local data storage can make personal data more susceptible to inadvertent disclosures (i.e., data breaches) if the local data center is not committed to enacting best-in-class cybersecurity measures. Such inadvertent disclosures are the result of security failures. When it comes to data storage and protection, it is important the company involved (which either runs its own networks or uses a third-party cloud provider) be dedicated to implementing the most advanced methods to prevent such disclosures. The location of these systems has no bearing on the security of data.¹⁴⁶⁶

Concern has been expressed that those responsible for a transborder data transfer might seek to avoid data protection controls by moving their operations, in whole or in part, to “data havens”, i.e., to countries which have less strict data protection laws, or none.¹⁴⁶⁷ However, one must also acknowledge, that a data protection law applicable to a specific data processing scenario might not be easily ascertainable. For companies operating in Europe and third countries, it has become a considerable effort to respect different data protection standards for different regions. Moreover, compliance with such standards might be incompatible with domestic law. International cooperation in the field of data protection to avoid such unequal treatment up to discrimination has so far hardly been progressive; especially in the transatlantic relationship, where European and US ideas on ensuring an adequate level of protection still prove to be different.

Accordingly, control concepts were considered for transborder data flows. The object of what was to be “controlled” was the “circumvention of the law”. Kuner stated that “the term could be used in a subjective sense, such as when a party transfers data with the primary purpose of evading application of the law, or in an objective sense, such as when the primary purpose of transferring the data is a business factor (e.g. optimization of

¹⁴⁶³ GSMA. (September 2018). *Cross-Border Data Flows Realizing benefits and removing barriers*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf. P. 14.

¹⁴⁶⁴ Kuner, C. [Christopher]. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD iLibrary, No. 187*. <https://doi.org/10.1787/5kg0s2fk315f-en>. P. 23–24.

¹⁴⁶⁵ Ustaran, E. [Eduardo]. (16 June 2022). *In search of a data localization strategy*. <https://www.linkedin.com/pulse/search-data-localization-strategy-eduardo-ustaran>.

¹⁴⁶⁶ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

¹⁴⁶⁷ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 130.

business processes, cost considerations, factors relating to IT infrastructure, etc.) other than evasion of the law”¹⁴⁶⁸. Within the European framework, the primary goal of the rules to prevent circumvention was recognized by Directive 95/46 and repeated in the GDPR. In *Schrems I*, the CJEU held that adequacy decisions under Directive 95/46 aim to prevent the circumvention of the high level of protection by transferring personal data outside the EU/EEA. In *Schrems II*, the CJEU added to this interpretation that an adequate level of protection is only given if it is “essentially equivalent” to that of the Union. The EU therefore set standards with an impact beyond its territorial borders. Due to the US legal framework differing from the European level of protection of personal data, practically every insistence from Europe could possibly be justified with the intention to avoid a circumvention of the law and ultimately to protect EU citizens. There are therefore constant fears in the US of a wide reach of European data protection law,¹⁴⁶⁹ most recently heightened by the decisions of European SAs on the use of Google Analytics.¹⁴⁷⁰ The transatlantic disputes about data protection became evident when the impact of data protection regulation could not be limited to the territory of the originating jurisdiction and State capabilities and authorities in other jurisdictions were “constrained to the point where impacts cannot be mitigated”¹⁴⁷¹. US government and US business representatives have repeatedly claimed that the level of protection in the US is at least on par with the European framework, if not more effective. It is true that US State level legislation, such as the CPRA, has a considerable number of adequate protections in place, but there are still shortcomings in many US States and at US federal level, as *Schrems II* confirmed.¹⁴⁷²

It must therefore be addressed whether the EU is pursuing good practice from a global perspective with the adequacy principle, or whether this could be classified as provocative behavior under international law. The system of legal instruments for establishing an adequate level of protection combined with the high assessment criteria for adequacy promotes the worldwide respect of the right to data protection as a universally applicable human right. This also led to the designation of the GDPR as the “gold standard” and the EU the *de facto* worldwide standard regulator in data protection law.¹⁴⁷³ In a keynote, Peter Schaar, retired German Federal DPO, asked to which extent the GDPR is developing into such standard, against which data protection worldwide should then be measured, noted that it is undisputed that European data protection law has moved in the right direction and that large international groups can nowadays no longer ignore it.¹⁴⁷⁴ The CPRA with strong similarities to the GDPR, and the statement by Apple CEO Tim Cook, who described the GDPR as a role model for global data protection,¹⁴⁷⁵ indicate that the GDPR has a global impact as a reference for adequate protection. With the help of the adequacy principle, the level of protection can potentially be maintained even beyond the EU borders. However, this is offset by the considerable resources required and the enforcement difficulties. The relatively small number of 14 adequacy decisions by the Commission can be explained by the fact that the assessment of the data protection level of an entire national legal framework is complex and time-

¹⁴⁶⁸ Kuner, C. [Christopher]. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD iLibrary, No. 187*. <https://doi.org/10.1787/5kg0s2fk315f-en>. P. 23.

¹⁴⁶⁹ CNET. (2 January 2022). *Congress fears European privacy standards*. <https://www.cnet.com/tech/services-and-software/congress-fears-european-privacy-standards>.

¹⁴⁷⁰ See Chapter II, Section II.3.4.4.g.

¹⁴⁷¹ Kobrin, S. [Stephen]. (2004). Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 30(1), 111–131. P. 111.

¹⁴⁷² See also Chapter IX, Section III.2.; and Chapter IX, Section III.3.

¹⁴⁷³ European Commission. (28 January 2014). *Speech: A data protection compact for Europe*. https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_14_62.

¹⁴⁷⁴ Keller, A. [Anja]. (2019). Tagungsbericht: PinG-Jahrestagung Datenschutz. *Kommunikation & Recht*, 2019(4), P. IX.

¹⁴⁷⁵ Baraniuk, C. [Chris]. (24 October 2018). Tim Cook blasts ‘weaponization’ of personal data and praises GDPR. *BBC*. <https://www.bbc.com/news/technology-45963935>.

consuming.¹⁴⁷⁶ The adequacy principle, however, neither directly interferes in the affairs of third countries, nor tangentially affects their sovereign rights. It is comprehensible that the level of protection set by the GDPR “gold standard” could appear presumptuous from a non-European perspective, if not as an abusive pressure to act and adapt to. However, the objective of fundamental rights protection confirmed by the GDPR as the basis for European data protection law makes an extension of protection beyond EU national borders justifiable. Nor can it be in the interest of international law to prevent practices that serve the effective protection of a nationally and internationally recognized fundamental rights. Nevertheless, the adequacy principle remains a threat to the goal of a free flow of data. The reaction of a third country is either to adopt the European level of protection or to insist on its own understanding of this level, which can lead to legal and factual burdens for the global digital economy based on transborder data flows, as shown in particular in the arena between the EU and the US.¹⁴⁷⁷

The tendency towards extraterritorial reach of legislation makes it clear that threats to fundamental rights by foreign States can also have effects for data subjects that are supposedly subject to their domestic law only. Particularly assertive (associations of) States such as the EU or US are increasingly willing to waive conventional forms of bilateral action, such as MLATs, to fasten the enforcement of their interests regardless of jurisdictional conflicts and the sovereignty of other States. The scope of European data protection regulations does not discriminate third-country nationals, as “data subjects in the Union” means any person in the Union whose information is being collected at that moment, regardless of their nationality or legal status. On the other hand, US law in some cases refers to the nationality of the person concerned. US law provides privileges for US citizens if personal data are processed in connection with intelligence actions abroad.¹⁴⁷⁸ As already shown in connection with the NSA’s PRISM program, this led to discrimination against foreign citizens, and – as Kuner noted –, in some cases to the enactment of “transborder data flow regulation because of concerns about data processing risks in other countries”¹⁴⁷⁹. This concerns not only data protection, but also aspects of data security, as a study noted: “Data may be processed in countries that do not have equivalent privacy regulation in place and could be more vulnerable to hacking.”¹⁴⁸⁰

Another point worth mentioning besides adequacy is a gap in coverage. Chapters II–VII described that a patchwork of data protection regulations exists at global level. This patchwork leads to gaps in coverage. Associated negative effects can even be measured in monetary terms, using two studies as examples. The “European Centre for International Political Economy” (ECIPE) stated that

if services trade and cross-border data flows are seriously disrupted (between the EU and U.S.), the negative impact on EU GDP could reach -0.8% to -1.3%. EU services exports to the United States drop by -6.7% due to loss of competitiveness. As goods exports are highly dependent on efficient provision of services (up to 30% of manufacturing input values come from services), EU manufacturing exports to the

¹⁴⁷⁶ Kuner, C. [Christopher]. (2009). Developing an Adequate Legal Framework for International Data Transfers. In S. [Serge] Gutwirth and Y. [Yves] Pouillet and P. [Paul] de Hert and C. [Cécile] and S. [Sjaak] Nouwt (ed.), *Reinventing Data Protection?* (pp. 263–275), Springer. P. 263.

¹⁴⁷⁷ See also Chapter IX, Section II.1.

¹⁴⁷⁸ See also Chapter III, Section II.1.

¹⁴⁷⁹ Kuner, C. [Christopher]. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD iLibrary, No. 187*. <https://doi.org/10.1787/5kg0s2fk315f-en>. P. 23.

¹⁴⁸⁰ GSMA. (September 2018). *Cross-Border Data Flows Realizing benefits and removing barriers*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf. P. 10.

United States could decrease by up to -11%, depending on the industry. In such case, the export benefits produced by the EU-U.S. FTA are eradicated by a good margin.¹⁴⁸¹

This disruption¹⁴⁸² has so far come from *Schrems I* and *Schrems II*, and if coverage in the US and the Union continue to differ, further disruption could be imminent. Castro / Dascoli / Diebold noted for gaps within US legislation that

for both the economy at large and small businesses, a 50-state privacy patchwork levies greater costs through a system of duplicative compliance and enforcement than through in-state costs alone. [...] Poorly designed data privacy laws can impose a substantial toll on the economy through both direct compliance costs and indirect costs from lower productivity and constraints on innovation; and when multiple states subject businesses to conflicting privacy laws, they increase these costs.

II. Different approaches to the nature and scope of the right to data protection

In the previous Section, we considered the problem drivers consisting of (i) restrictions imposed for the sake of national digital economy policy, and (ii) the balance between the interests of data protection and national security / public order. In this Section II, we will explore three more problems drivers, which relate to conflicting conceptions of the nature and scope of the right to data protection. Firstly, that the legal nature of the right to data protection is still widely discussed and can range between a human right, a position in consumer law to regulate market-driven aspects, and an ownership right. Secondly, that the right to data protection in national laws is often balanced differently with conflicting guarantees in other fundamental rights. Lastly, that the scope of the right to data protection might be questionable.

While States were able to ensure compliance with fundamental rights positions in the analogue world, this has proven to be challenging in transborder data transfer situations. In this respect, the question arises whether it is necessary to further develop areas of fundamental protection to achieve an effective legal order. These cases encompass, on the one hand, the protective dimension of fundamental rights, which is concerned with whether and to what extent the fundamental rights holder can demand measures from the State that prevent third Parties from affecting its fundamental rights. On the other hand, in constellations that relate to the private law relationships, the question of whether and to what extent private individuals are subject to fundamental rights obligations triggers then indirect third-party effects. Since the fundamental guarantee of human dignity is increasingly mentioned in the public debate as the starting point for the right to data protection, this aspect must be considered. Despite the frequent connection between data protection and human dignity (in Germany, for example, manifested in Art. 1(1) *Grundgesetz*), most of the Internet-related cases do not affect human dignity itself. A differentiation between general personality rights (Art. 2 (1) *Grundgesetz*) and human dignity becomes then necessary. The State, reacting to the scope of the right to data protection in question, then usually has a wide margin of discretion. The possibilities of the State are on the one hand to strengthen the relevant dimensions of effectiveness by means of an increased constitutional specification or the first-time representation in the constitutional text. On the other hand, the State could sharpen which administrative

¹⁴⁸¹ ECIPE. (March 2013). *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*.
https://www.uschamber.com/assets/archived/images/documents/files/020508_EconomicImportance_Final_Revised_Ir.pdf. P. 3.

¹⁴⁸² Although ECIPE did not define what they considered being a "serious" disruption.

measures are appropriate or constitutionally required to fulfill the constitutional protection mandate. Given the wide scope of legislative and administrative design, both legal and factual measures can be considered as such. A mix of measures from different components could be a useful variant. Those were outlined in Chapter VI, Section II.

At the international law level, the right to data protection is codified in Art. 17 ICCPR, which forms the binding version of the non-binding Art. 12 UDHR. Both the ECtHR and the CJEU recognize the protection of personal data as a fundamental right. This case law was initially based on Art. 8 ECHR. In the meantime, however, the EU has also acknowledged the protection of personal data by Art. 8 of the Charter.

The OECD found that “the approach to privacy and personal data protection varies across cultures, which is why regulation also differs”¹⁴⁸³ and that “privacy itself is difficult to define. It means different things to different people [...] and the value we attach to privacy, whether as individuals or in society, can be subjective [...]”¹⁴⁸⁴ On the Internet, the different cultural values now come together; a “clash of values” occurs.

Common law, on which the law of the US is based, traditionally knew no right to data protection. For a long time, US law followed this approach and only granted protection of personal data limited to the area of honor protection through the torts libel and slander, which are grouped under the generic term “defamation” and only protect against defamatory content of written and oral statements. The first impetus to put data protection on a broader basis came from Warren / Brandeis, which was revolutionary for the time because it led to common law recognizing the overriding legal principle of right to privacy.¹⁴⁸⁵ Today, all States in the US recognize a right to data protection, albeit to different extents, either because of common law, because of special regulations, or because of both. In 1960, Prosser noted that the right to privacy cannot be clearly defined due to its vagueness, and that an idea of its concrete content can only be obtained empirically by structuring and systematizing the decided legal cases.¹⁴⁸⁶ The essay underwent a detailed analysis of case law. According to his classification, which is generally followed in case law and literature today, there are four case groups: intrusion cases, public disclosure cases, false light cases, and appropriation cases.

Among the various interests against which the right to data protection must be weighed and which limit its scope, one interest stands out because of its fundamental sociopolitical importance, namely the right to freedom of expression, as stated in the First Amendment of the US Constitution. A collision between the interests of the individual to have their personal data protected and the public’s need for information naturally occurs in cases that fall under the second group of Prosser’s classification, i.e., the publication of embarrassing facts from private life. In general, courts tend to subordinate personal protection to the general interest in free reporting.¹⁴⁸⁷ This applies at least when it comes to information about people who are in public life, so-called “public figures”. This attitude is justified by the fact that those who voluntarily expose themselves to the public eye, largely forego the protection of their personal data and therefore must accept that reports about their private lives are reported. Insofar as it concerns persons who have come into the public eye against their will, their right to data protection is largely replaced by the right to know of the public (“right to know”), which in the US view is to be interpreted broadly and is not limited to the event as such, but also extends to details from the private

¹⁴⁸³ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 14.

¹⁴⁸⁴ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 31.

¹⁴⁸⁵ Brandeis, L. [Louis] and Warren, S. [Samuel]. (1890). *The Right to Privacy*. *Harvard Law Review*, 4(5), 193–220.

¹⁴⁸⁶ Prosser, W. [William]. (1960). *Privacy*. *California Law Review*, 48(3), 383–423.

¹⁴⁸⁷ McCarthy, J. T. [J. Thomas]. (1994). *The Rights of Publicity and Privacy*. Clark Boardman Callaghan. § 5.9 [B].

life of those involved.¹⁴⁸⁸ Ultimately, whether and to what extent personal data may be revealed, depends on whether its disclosure is of matters of legitimate concern to the public. However, all these are not assessment criteria, but rather case law in the US reacting to actual circumstances on a case-by-case basis.

In Europe, there were different ideas about the sensitivity of personal data until the harmonization set forth through Directive 95/46 and GDPR. France had the idea that trade union membership and philosophical convictions were among the most sensitive data to be protected. In Switzerland, people were very sensitive about data on the receipt of social benefits. The debate over the legal development of data protection went along with the relationship between the right to respect for private life, and the right to data protection, culminating in its enshrinement in Art. 8 of the Charter, and in the data subject's rights granted by the GDPR. The application of Arts. 52(3) and 53 of the Charter encountered difficulties whilst balancing fundamental rights relationships, where data protection on the one hand and freedom of the press on the other hand are in conflict. In these cases, one fundamental right applies at the expense of the other fundamental right, so that a minimum level of fundamental rights cannot be determined immediately. It is ultimately up to case law to find a balance between these fundamental rights concerned. In several judgments, the ECtHR dealt with the trade-off between data protection in Art. 8 ECHR on the one hand and the rights guaranteed in Art. 10 ECHR on the other. The ECtHR regularly emphasized the importance of freedom of expression¹⁴⁸⁹ and freedom of the press¹⁴⁹⁰ for every democratic society, but at the same time demanded a legitimate public interest in reporting, which it tended to deny in the case of mere tabloid reporting. Rather, the statement included in Art. 10 ECHR must contribute to a debate of general interest. According to the ECtHR, neither Art. 8 ECHR nor Art. 10 ECHR have priority over the other fundamental right.

In yet another manifestation of conflicting views on the nature and scope of the right to data protection, in the last years, legal experts have been arguing about the topic of “data ownership”. Janeček maintained comprehensibly that, until the necessary technological advancements are available, ownership-like protection of personal data will remain fragmented. He argued that until such advancements eventuate, full ownership of personal data will remain both technologically and legally unresolved.¹⁴⁹¹ Drexl similarly found that “calls to complement the data protection rules of the GDPR with an economic data ownership right held by the data subject should be rejected”¹⁴⁹². He argued further that the proposals, which were also driven by the normative object of property (“*bien*”) existing in civil law in France

are affected by essentially two major fallacies. First, these proposals neither take into account the impact of such ownership on the functioning of data markets nor do they explain the need for the recognition of an additional intellectual property right in the light of a market-failure analysis. Secondly, the claim that the data subjects should own their data and have full control over the commercialization of their data begs the question of whether the privacy interest underlying the data protection rules of the GDPR also extends to such broader economic interests. According to the regulatory theory advocated here, a clear distinction should be drawn between the personality interests of the data subject and ownership rights as a tool of market regulation. Otherwise, legislation on data ownership of the data subject in personal data would run the risk of

¹⁴⁸⁸ McCarthy, J. T. [J. Thomas]. (1994). *The Rights of Publicity and Privacy*. Clark Boardman Callaghan. § 5.9 [B].

¹⁴⁸⁹ ECtHR, *Handyside v. UK*, Application no. 5493/72, (7 December 1976).

¹⁴⁹⁰ ECtHR, *Caroline von Hannover v Germany*, Applications no. 40660/08 and no. 60641/08, (7 February 2012).

¹⁴⁹¹ Janeček, V. [Václav]. (2018). Ownership of Personal Data in the Internet of Things. *Computer Law & Security Review*, 34(5), 1039-1052.

¹⁴⁹² Drexl, J. [Josef]. (2019). Digital economy and the disruption of traditional concepts. In A. [Alberto] De Franceschi and R. [Reiner] Schulze, *Digital Revolution - New Challenges for Law* (pp. 19–40). Nomos. P. 31.

being adopted without the necessary balancing, with potential negative effects on the working of data markets. However, to conclude that the data protection rules of the GDPR should not be complemented by data ownership of the data subject still requires additional arguments. [...] Member States cannot be considered to have the power to adopt legislation on a data ownership right of the data subject by only relying on the fundamental right to data protection.”¹⁴⁹³

Trakman / Walters / Zeller noted that it is nevertheless important

to address the extent to which personal information and data ought to be treated as property, and as IP rights in particular. The ability to balance the rights and control of data subjects against the rights of data users, is an unavoidable challenge for regulators and policy makers. How much control ought to be afforded to data subjects through the law is contentious. Whether that control extends to the first, second, third, fourth, fifth, or further point in the cycle of collection and use of personal data is an open question. The principles espoused by the OECD, particularly regulating transparency in data use and accountability for its misuse, provide a sound point of commencement. The issue is to determine how far they ought to be extended. These are also policy challenges that warrant ongoing scrutiny, such as how the regulation of personal data ought to reconcile private data rights with public interests in that data.¹⁴⁹⁴

The EU Commission therefore intended to create clear rules for data markets with its “data producer right”¹⁴⁹⁵. The question arises whether data subjects should be given a financial contribution to the profits generated by their personal data. A possible right to data would need not necessarily be an all-encompassing, property-like law. Likewise, it could be possible to think about access rights to data or to assign individual authorizations sector-specifically. As an alternative to a right to data, contractual clauses could also distribute the powers of personal data in an appropriate way. From an economic point of view, an at least proportionate right to the data value could also be assigned to the person who issues the data and makes it commercially usable.

At national level, in German law, e.g., ownership can only exist on movable and immovable property or animals according to § 90 BGB and § 90a BGB. According to the legal definition of § 90 BGB, things are physical objects. In principle, non-physical objects are not things and cannot be property. Data are immaterial and cannot be consumed. § 90 BGB therefore in principle does not include any data. There is therefore no ownership of data according to § 903 BGB. This basic position in civil law led to the question: “Who owns data?” Ownership works absolutely, so towards everyone (*erga omnes*). Ownership of personal data on the one hand and data independent of a personal reference on the other should be considered. In the German legal-political landscape, demands on the legislator to regulate this issue more precisely have become louder, which is why the working group “Digital Restart” of the Justice Ministers of the federal States dealt with the topic in 2017.¹⁴⁹⁶ The report resumed nevertheless, that the creation

¹⁴⁹³ Drexl, J. [Josef]. (2019). Digital economy and the disruption of traditional concepts. In A. [Alberto] De Franceschi and R. [Reiner] Schulze, *Digital Revolution - New Challenges for Law* (pp. 19–40). Nomos. P. 34.

¹⁴⁹⁴ Trakman, L. [Leon] and Walters, R. [Robert] and Zeller, B. [Bruno]. (2019). Is Privacy and Personal Data Set to Become the New Intellectual Property?. *International Review of Intellectual Property and Competition Law*, 937–970, <http://dx.doi.org/10.2139/ssrn.3448959>. P. 965.

¹⁴⁹⁵ European Commission. *Building a European Data Economy*, COM(2017) 9 final, (10 January 2017). P. 13 ff.

¹⁴⁹⁶ Konferenz der Justizministerinnen und Justizminister der Länder, Arbeitsgruppe “Digitaler Neustart”. (15 May 2017). *Bericht vom 15. Mai 2017*.

https://jm.rlp.de/fileadmin/mjv/Jumiko/Fruhjahrenskonferenz_neu/Bericht_der_AG_Digitaler_Neustart_vom_15._Mai_2017.pdf.

of such an absolute right is neither necessary nor desirable.¹⁴⁹⁷ It found that although the protection of digital data in the legal system is more of a patchwork, there are no significant gaps in protection. The protection that currently results primarily from criminal and property law provisions as well as from special laws on data content (e.g., copyright) is sufficient to adequately reconcile the conflicting interests. Despite this clear (German) position there are still proposals to expand civil law with a property- and intellectual property law approach to digital data law. The US has also not yet created such a data ownership regime.

China is increasingly taking a different position. Boullenois found that “Chinese policymakers are now starting to call for a legal system that creates and defines data property rights, thus allowing data to become a tradable commodity that can be bought and sold on data trading platforms.”¹⁴⁹⁸ China believes since its 14th five-year plan¹⁴⁹⁹ that this should be achieved through “non-exclusivity and multistakeholder joint ownership, with different data subjects and data processors exercising different rights over data according to their role in generating, maintaining and using it”¹⁵⁰⁰.

It is still largely unclear to whom the data “belongs” to, which part and which value is to be given to each part. For example, a distinction could be made between the customer who provides personal data and is protected by data protection law (as a defense right) and the company having power over the personal data under its control. In China, it was therefore discussed which ownership rights should be assigned to those responsible for a data processing and which to the data subjects. There would be the possibility to reserve a “data ownership rights *sensu stricto* [...] to large databases held by businesses and not extended to individuals’ personal data. This would mean that those responsible would get – under certain conditions – the rights to manage, use and derive income from the data they held, but individuals would not be able to monetize or derive income from their personal information.”¹⁵⁰¹

Discussions among scholars and policymakers have essentially crystallized two main arguments. Proponents of a data ownership regime argue that it would create incentives to generate and share data; critics argue that it would stifle the growth of the digital economy, hinder the movement of data and accelerate data monopolization.¹⁵⁰² Aaronson noted that, “if regulators view data as a form of property, corporations would have to pay for permission, pay to collect and use data, and no longer offer services for free. Moreover, [...] if firms are required to pay to use personal data, they would have an incentive to keep data accurate and carefully stored.”¹⁵⁰³ On the other hand, even if data

¹⁴⁹⁷ Similarly, the German Data Ethics Committee stated that “such a contribution to the generation of data should, in the view of the Data Ethics Committee, however, not lead to exclusive property rights to data, but rather, if necessary, to data rights in the form of special participation rights of an actor, with corresponding obligations of other actors.” See German Federal Ministry of the Interior. (10 October 2019). *Gutachten der Datenethikkommission*. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6. P. 17.

¹⁴⁹⁸ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 3.

¹⁴⁹⁹ Costigan J. [Johanna] and Webster, G. [Graham] (eds.). (March 2021). *14th five-year plan for the national economic and social development of the People’s Republic of China and the outline of long-term goals for 2035*. <https://digichina.stanford.edu/wp-content/uploads/2022/01/DigiChina-14th-Five-Year-Plan-for-National-Informatization.pdf>.

¹⁵⁰⁰ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 3.

¹⁵⁰¹ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 3.

¹⁵⁰² Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 3.

¹⁵⁰³ Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 6.

subjects are treated as legal owners of their personal data and “enjoy negative rights”¹⁵⁰⁴ similar to the data subject rights in the GDPR, they are unlikely to ever identify whether their ownership has been violated. Each time a contract is concluded, there would be a need to clarify whether the alleged data owner is also entitled to grant access and transfer this property. This could be avoided if data could be contractually protected by non-disclosure agreements, which could include a contractual penalty. It is also argued that due to the lack of physicality of the data, property rights only arise on data carriers on which they are located.¹⁵⁰⁵ However, today’s technical progress means that data carriers are hardly used anymore, thus data could also be seen as a form of infrastructure environments increasingly depending upon data in real-time.

Moreover, when creating a right, the scope of protection would also have to be determined. This would require a precise definition of the complex term “data”.¹⁵⁰⁶ Carvalho / Kazim therefore understandably called for prioritization of data standardization.

If data are to be considered an economic asset, it must be carefully and completely described: data formats, data quality metrics, data usability conditions, data sources qualification, and other data properties must be collected in the metadata. Equally important is understanding data value, data use terms and conditions and to create a common taxonomy. Quantitative metrics to assess potential of data are needed. Risk assessment models are also needed.¹⁵⁰⁷

China seems to follow this goal with a synchronized approach based on different measures. China tends “to envisage significant powers for the state as a key regulator and actor in data collection and sharing. Policymakers and experts are exploring different paths to encourage – or force – companies to grant the government access to their data resources, for example tax deduction policies for companies willing to share data or financial compensation for mandatory data sharing.”¹⁵⁰⁸ In this system, the stakeholders are the government, the citizens, and companies, as the following graphic shows.

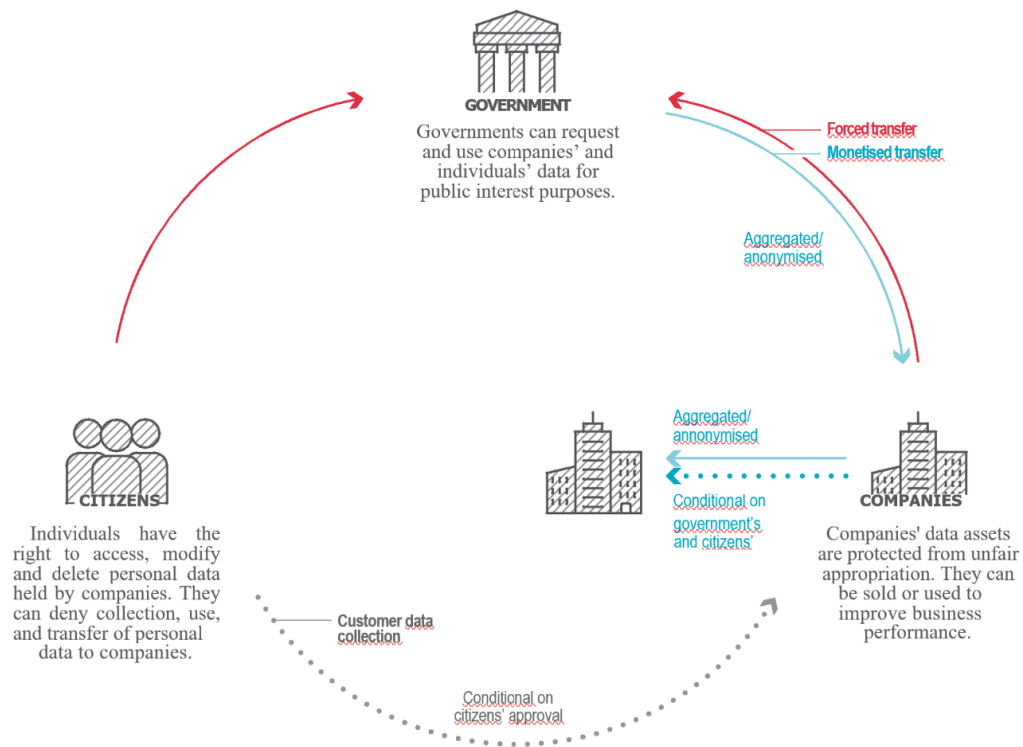
¹⁵⁰⁴ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 3.

¹⁵⁰⁵ Roßnagel, A. [Alexander]. (2014). Fahrzeugdaten – wer darf über sie entscheiden?. *Straßenverkehrsrecht*, 2014(8), 281–287. P. 282 f.

¹⁵⁰⁶ Drexl, J. [Josef] and Hilty, R. [Reto] et al. (16 August 2016). *Ausschließlichkeits- und Zugangsrechte an Daten, Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb vom 16. August 2016 zur aktuellen europäischen Debatte*. https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI-Stellungnahme_Daten_2016_08_16_final.pdf. P. 4.

¹⁵⁰⁷ Carvalho, G. [Graca] and Kazim, E. [Emre]. (2022). Themes in data strategy: thematic analysis of ‘A European Strategy for Data’ (EC). *AI and Ethics*, 2(2), 53–63. P. 54.

¹⁵⁰⁸ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 4.



Source: Boullenois, Camille, "Rights and transfers in China's emerging data governance regime between government, companies and citizens"¹⁵⁰⁹

PIPL, as one piece in this system, grants substantive protection for data subjects. However, these would "not be able to monetize or derive income from their personal information, but they would enjoy negative rights, for example the rights to refuse to grant authorization to use their information, to delete it, to access it or to rectify it"¹⁵¹⁰. Ownership rights should only apply to "large databases". This would result in companies enjoying "the rights to manage, use and derive income from the data they held – under certain conditions"¹⁵¹¹. On the one hand, these conditions are derived from PIPL, which mainly refers to consent in the lawfulness of processing, but also to other grounds, Art. 13 PIPL. Since these conditions are similar in strength to those of the GDPR, a horizontal flow of personal data between citizens and companies is limited. On the other hand, these conditions are derived from the CSL, which requires such companies to improve the security of their data networks, and the DSL, which protects national data resources. In the context of the CSL, and most notably the DSL, China is using *de facto* "forced transfers" as means to place the government at the fulcrum of this system.¹⁵¹² With the so-called "Shenzhen regulation", the first of its kind to be passed by a local government in China and effective since 1 January 2022, three different data rights were defined for the first time for three different stakeholders in this system:

The personal data rights enjoyed by individuals obey a different logic from ownership rights – they are civil rights as defined in China's Civil Code. By comparison, companies enjoy rights closer to traditional ownership rights. They can buy and sell legally obtained

¹⁵⁰⁹ Boullenois, C. [Camille]. (October 2021). China's Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 3.

¹⁵¹⁰ Boullenois, C. [Camille]. (October 2021). China's Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 4.

¹⁵¹¹ Boullenois, C. [Camille]. (October 2021). China's Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 3.

¹⁵¹² Boullenois, C. [Camille]. (October 2021). China's Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 4.

data through legally established data trading platforms. The Shenzhen regulation also defines public data as a new type of state-owned asset, held and collected by government authorities and public institutions [...]. Individuals and companies whose data are being collected by the state must comply, although they may raise objections if they believe the data collection is inaccurate or infringes on their personal privacy, business secrets or other legitimate interests. Some of this public data, then, is to be provided free of charge to the public, while some will be conditionally open or for state use only.¹⁵¹³

If the goal of capturing the divergent variety of data would be envisaged through an abstract definition, this new data right could lack a clear demarcation. In addition, ownership of data would not be exclusive. The same data could be assigned more often. Functionally, data are therefore more closely related to licenses. Multiple licenses could be granted on the same data. Moreover, the misuse of data can already be punished by means of GDPR or other standards under applicable law. Standards against unfair competition do not create exclusive rights, rather they prohibit certain actions by market participants. This leads already to a high degree of application flexibility and the access to data remains open for companies. If ownership of data would be created, companies and private individuals could lose it through foreclosure. In addition, liens or security rights could arise on data. If more than one person owns the data, a collective community could arise. It would also be questionable whether it is possible to acquire data in good faith, on which element of data this good faith and thus the protection of legitimate expectations of the purchaser should be based. Plus, data exchange and the use of the Internet are not territorial as data paths cross borders. Assigning an exclusive ownership right could result also in problems with applicable law, provisions in the Rome I¹⁵¹⁴/II¹⁵¹⁵ and Brussels I¹⁵¹⁶ regulations would have to be adapted. Moreover, the creation of data ownership should not weaken legal certainty. In the area of data markets, however, this weakening could happen due to the difficulties mentioned above. To date, the transfer of data has also worked without ownership of the data and the trade of data does not necessarily require a legal assignment of data. Overall, it is not evident that creating an ownership of data is currently necessary, and – with Aaronson – personal data should be seen as “a by-product of our thinking, actions and simply living. It is not one thing; thus, we should not simply view it as a resource, or as property, capital, labor or infrastructure.”¹⁵¹⁷

Although the idea of a “data producer right” and financial compensations for data subjects emerged in 2017, the economic allocation of data - in the absence of data ownership - could only take place on a voluntary contractual basis, with extensive contractual freedom applying to date. The proposed Data Act¹⁵¹⁸ of 2022 has the potential to change the Commission’s approach to this ownership right and the legal framework of the data economy; it remains to be seen how this proposed Act will evolve. In the sense of a uniform legal system, it is nevertheless essential to dogmatically classify the ownership of data to solve borderline cases and to answer questions of current law

¹⁵¹³ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 5.

¹⁵¹⁴ EC. *Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)*, OJ L 177/6, (4 July 2008).

¹⁵¹⁵ EU. *Regulation (EU) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II)*, OJ L 199/40, (31 July 2007).

¹⁵¹⁶ EU. *Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters*, OJ L 351/1, (20 December 2012).

¹⁵¹⁷ Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 6–7.

¹⁵¹⁸ See Chapter II, Section II.3.8.2.

in a stringent way. In addition, new terminology is also necessary to bring the open discussions, which are often lost in the supposedly legal-free vastness of the global network, to a sensible end.¹⁵¹⁹ The Max Planck Institute for Innovation and Competition also described a possible pathway:

Information should not be subjected to a general property right without specific justification, such as in the case of patent law. [...] The focus is not on a general “data ownership right”. Because a data traffic as unhindered as possible is not dependent on ownership rules, but rather access rules. The debate about this should be conducted intensively. Specific rules are also conceivable in specific sectors in which there are particular problems due to lack of access to data.¹⁵²⁰

III. Extraterritoriality and blocking statutes

The legend of an uncontrollable cyberspace ignores that jurisdiction can also extend to TFPD scenarios, and that the technological progress enabled data localization possibilities¹⁵²¹. This led to an increasing split between the nationality of a data subject and a legal system applicable to those responsible for the data processing in such a scenario. Territorial concepts are somewhat ineffective in a structure that is not spatially organized. Since different frameworks have chosen different approaches, it can occur that two States side by side declare to have jurisdiction over such scenario. There are historical reasons for this. In an early phase, various forms of private autonomy regulation of the Internet were discussed¹⁵²², and it was no uncommon idea that the Internet is so fundamentally different to former systems, that it needed new rules; the principle of territoriality was questioned, especially in relation to governmental surveillance and “big data”.¹⁵²³

A location-flexible data processing goes hand in hand with uncertainties regarding the application of a law. Associated enforcement problems¹⁵²⁴ led to gaps in protection¹⁵²⁵ for data subjects. For regions such as the EU, which applies a high level of data protection, it is difficult to maintain this level whenever a TFPD scenario applies. One solution to this is for such States to seek an extension of their own legal order by enacting regulation with extraterritorial effect. The aim hereby is to extend the scope of application of own regulations so that, from a national perspective, these rules can resolve scenarios with a global reach without having to stop at national borders. It is hence important for a State to consider the interests of its own data processing economy and to promote its development, while at the same time ensuring effective data protection adapted to the level of protection accepted by its population. This can lead to conflicts at the international level which are to be discussed in this Section III.

The starting point of those considerations by States lies on the principle of territoriality, which is derived from State sovereignty. A State can issue regulations based on its own territory. The regulation of extraterritorial matters needs to be justified insofar as it interferes with another State sovereignty, which in turn is also territorially determined.

¹⁵¹⁹ European Commission. *Trade for All Towards a more responsible trade and investment policy*, COM (2015) 497 final, (14 October 2015). P. 7.

¹⁵²⁰ Max Planck Institute for Innovation and Competition. (1 August 2017). *Argumente gegen ein “Dateneigentum”*, 10 *Fragen und Antworten*.

https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf. P. 4.

¹⁵²¹ See Chapter VIII, Section I.

¹⁵²² Engel, C. [Christoph]. (21 August 2002). *The Role of Law in the Governance of the Internet*.

<http://dx.doi.org/10.2139/ssrn.325362>. P. 201 ff.

¹⁵²³ Johnson, D. R. [David Reynold] and Post, D. [David G.]. (1996). Law and Borders - the Rise of Law in Cyberspace. *Stanford Law Review*, 48(5), 1367–1402. P. 1367 ff.

¹⁵²⁴ See Chapter VIII, Section I.2.

¹⁵²⁵ See Chapter VIII, Section I.3.

This results in the need to differentiate sovereign powers from one another. This delimitation is complicated by the plurality of State jurisdictions, i.e., that different jurisdictions may compete and overlap. This could be mitigated by separating the jurisdiction to prescribe from the jurisdiction to enforce. At the latest when it comes to the question of the enforcement of its data protection law, each State must respect territorial boundaries.

International law itself does not prohibit a State from regulating actions, persons, or objects outside its own territory, even if territorial sovereignty was the basis for national legislation. The ICJ's S.S. *Lotus* decision¹⁵²⁶ granted a State a fundamental discretion to decide on the territorial extent of its jurisdiction. Although the court did not concretize the limits of such discretion, further ICJ cases emphasized the need for a "genuine link" between the subject matter of the jurisdiction and the territory of the State seeking to exercise its jurisdiction.¹⁵²⁷ To determine this link, it is necessary to resort to "connecting factors" that establish a relationship to the foreign facts, either indirectly or directly. In the area of data protection law, in particular the principles of territoriality, personality, and effects, are used for giving proof of this link.¹⁵²⁸

The principle of territoriality limits State legislation to a State's own territory with the actions, persons, or objects located therein. The principle of territoriality was found, e.g., in Art. 4(1)(c) Directive 95/46, where it referred to the use of equipment in the context of data processing activities. This was reiterated in Art. 3(1) GDPR, where the application of the GDPR is based on personal data being processed in the context of the activities of an establishment of a data controller or processor in the Union. A significant difference from Directive 95/46 now exists in Article 3(2) GDPR, from which stems "explicit or direct extraterritoriality".¹⁵²⁹ With its Art. 3(2), the GDPR broadened the *lex loci solutionis* principle and "outlines what types of contact with the EU's territory will activate the application of the GDPR, and it does so in a manner that is partly territoriality-dependent and partly territoriality-independent"¹⁵³⁰. A source of "indirect extraterritoriality"¹⁵³¹ of the GDPR had been developed in the CJEU's decisions in *Google Spain*, *Weltimmo*, *Verein für Konsumenteninformation*, and Facebook fanpages, in which the Court broadened its interpretation of Art. 4 Directive 95/46, bringing a non-EU controller within the grasp of EU data protection law. Although these cases were decided under Directive 95/46, they also have an impact on the interpretation of the GDPR, because Art. 3(1) GDPR corresponds to Art. 4(1)(a) Directive 95/46. Therefore Art. 3(2) GDPR could be seen as a bridge between Art. 4 Directive 95/46 and the new Art. 3 GDPR. A third way in which the European data protection regime has indirect extraterritorial impact are the effects of Chapter V of the GDPR. Through the "adequacy" (interpreted by the CJEU as "essentially equivalent") assessment, the Commission can deem a third country to be "adequate" within an adequacy decision. This led to non-EU states finding their domestic law and policy in the data protection arena "heavily influenced by EU law"¹⁵³², which

¹⁵²⁶ ICJ. S.S. *Lotus (France v. Turkey)*, 1927 P.C.I.J. (ser. A) No. 10, (7 September 1927).

¹⁵²⁷ "A State cannot claim that the rules it has laid down are entitled to recognition by another State unless it has acted in conformity with this general aim of making the nationality granted accord with an effective link between the State and the individual.", ICJ. *Nottebohm (Liechtenstein v. Guatemala)*, Summary of the Judgment of 6 April 1955, <https://www.icj-cij.org/public/files/case-related/18/2676.pdf>, (6 April 1955). P. 34.

¹⁵²⁸ Herdegen, M. [Matthias]. (2020). *Internationales Wirtschaftsrecht*. C.H. Beck. § 3, para. 52

¹⁵²⁹ Lynskey, O. [Orla]. (2021). Extraterritorial Impact Through an EU Law Lens. In F. [Federico] Fabbrini and E. [Eduardo] Celeste and J. [John] Quinn, *Data Protection Beyond Borders*, P. 193.

¹⁵³⁰ Svantesson, D. J. B. [Dan Jerker B.]. (2020). Art. 3. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 74–99). Oxford University Press. P. 76.

¹⁵³¹ Lynskey, O. [Orla]. (2021). Extraterritorial Impact Through an EU Law Lens. In F. [Federico] Fabbrini and E. [Eduardo] Celeste and J. [John] Quinn, *Data Protection Beyond Borders*, P. 194.

¹⁵³² Lynskey, O. [Orla]. (2021). Extraterritorial Impact Through an EU Law Lens. In F. [Federico] Fabbrini and E. [Eduardo] Celeste and J. [John] Quinn, *Data Protection Beyond Borders*, P. 196.

Bradford¹⁵³³ called “the Brussels Effect”. This has “global impact. Since they [territorial scope rules] apply its rules to data processing outside the territorial boundaries of the EU, they result in obligations for Parties engaged in such processing in third countries, including other countries themselves. Imposing such burdens results in the extraterritorial reach or territorial extension of EU data protection law, which risks conflicts with third countries”¹⁵³⁴. Already before the GDPR came into force, Bygrave called this “situation in which rules are expressed so generally and non-discriminately that they apply prima facie to a large range of activities without having much of a realistic chance of being enforced” as “regulatory overreaching”¹⁵³⁵. We agree with Kuner, who stated that the distinction between whether EU data protection requirements are “extraterritorial in scope” or “extraterritorial in effect” no longer has any practical significance. Regulation of data transfers under EU data protection law has become an extraterritorial jurisdictional regime, which is leading to increasing conflicts of law and greater difficulty in enforcing the law in a global context.¹⁵³⁶ Svantesson criticized this approach as going too far “thereby giving the GDPR a scope of application that is difficult to justify on the international stage, as the GDPR may end up applying in situations in relation to which the EU may be argued to lack a legitimate interest to apply its laws and to which it only has a weak connection”¹⁵³⁷. In a State-independent data structure of the Internet, the attribution of a TFPD scenario to an individual State has become even more difficult since personal data are transferred continuously transborder. National territory is no longer the only basis for establishing sovereignty; rather, due to globalization, the principle of territoriality is viewed increasingly critically as a criterion to delimit jurisdiction.¹⁵³⁸ Even if this principle seems to be unsuitable when considered on its own, it is not possible to completely abandon it. This is also shown by the rules of the GDPR, which combine the principle of territoriality with other connecting factors, although the legislator sees a smaller role in the principle of territoriality. Yet, the extraterritorial impact of EU data protection law is consistent with the corpus of EU law, the differentiation between TFPD within the Union and those beyond the EU’s borders can be justified on the basis of general principles of EU law.¹⁵³⁹

The principle of personality focuses on the connection between a State and its nationals. A distinction is made between the active and passive principle of personality. With the help of the active principle of personality, a State exercises power over its nationals even if they are abroad. A connection according to the passive principle of personality refers to the affectedness of own citizens abroad. In the current version of the GDPR, the principle of personality was ultimately not able to prevail. Domicile was not chosen as the connecting factor in the GDPR, but rather residence (“data subjects who are in the Union”). Choosing the principle of personality as the sole connecting factor could also lead to inadmissible interference in the affairs of a foreign State; if this principle would

¹⁵³³ Bradford, A. [Anu]. (2012). The Brussels Effect. *Northwestern University Law Review*, 107(1), Columbia Law and Economics Working Paper No. 533, <https://ssrn.com/abstract=2770634>.

¹⁵³⁴ Kuner, C. [Christopher]. (16 April 2021). Territorial Scope and Data Transfer Rules in the GDPR: Realizing the EU’s Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper No. 20/2021*, <http://dx.doi.org/10.2139/ssrn.3827850>. P. 11–12.

¹⁵³⁵ Bygrave, L. A. [Lee A.]. (2000). European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation. *Computer Law & Security Review*, 16(4), 252–257. P. 255.

¹⁵³⁶ Kuner, C. [Christopher]. (2015). Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. *International Data Privacy Law*, 5(4), 235–245. P. 236.

¹⁵³⁷ Svantesson, D. J. B. [Dan Jerker B.]. (2020). Art. 3. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 74–99). Oxford University Press. P. 95

¹⁵³⁸ Hörnle, J. [Julia]. (2021). *Internet jurisdiction*. Oxford University Press. P. 437. // Hörnle J. [Julia]. (26 March 2021). *Roundtable - Overcoming the Jurisdictional Challenge of the Internet?*. Queen Mary University of London, Centre for Commercial Law Studies. <https://www.qmul.ac.uk/ccls/events/past-events/videos-and-recordings/overcoming-jurisdictional-challenge-of-internet/>.

¹⁵³⁹ Lynskey, O. [Orla]. (2021). Extraterritorial Impact Through an EU Law Lens. In F. [Federico] Fabbrini and E. [Eduardo] Celeste and J. [John] Quinn, *Data Protection Beyond Borders*, P. 191–192.

had prevailed in the GDPR, the GDPR would also have been applicable in cases where a person domiciled in the EU is offered goods or services during a stay in a third country.

A State may also be entitled to link its regulatory sovereignty to the place of an event on its territory. The *lex loci solutionis*, in principle, is the law applied in the place of an event. In cases *Google Spain*, *Weltimmo*, *Verein für Konsumenteninformation*, and Facebook fanpages,¹⁵⁴⁰ the CJEU applied the *lex loci solutionis* to Directive 95/46. The GDPR added in Art. 3(2) GDPR the “targeting criterion” based on this *lex loci solutionis*. The GDPR applies therefore to data processing activities related to the offering of goods or services to data subjects in the Union. According to Recital 23 of the GDPR, this is the case if it is apparent that controller or processor envisage such an offer. For the territorial applicability of the GDPR it is therefore not necessary anymore that the controller or processor have a physical establishment within the Union.

Regardless of which connecting factor a legislature chooses, its choice must reflect a genuine link to its own State. Since two States could rely in TFPD scenarios on one and the same connecting factor and justify prescriptive jurisdiction, the “genuine link test” as to whether a State has a sufficient connection to the regulatory complex, minimizes weak territorial connections to inadmissible connecting criteria and thus the potential for conflict. The interests of other States must also be included in a final consideration, prior to exercise sovereignty. International law expects States to exercise this prudently and cautiously in cases in which several States can potentially claim the exercise of their own sovereignty (“comity analysis”).¹⁵⁴¹ A lack of such connection can lead to an excessive exercise of sovereignty, a so-called “jurisdictional overreach”.

Therefore, under certain conditions, States are allowed to adopt legislation that applies to scenarios taking place outside their territory. However, this does not mean that these laws can also be enforced outside their territory. Limitations to exercise sovereignty can stem from Art. 38(1) of the Statute of the ICJ. Based on this, a limitation could result from international conventions, international customs, or general principles of law. International conventions that explicitly concern the territorial scope of national regulations have not yet been concluded. However, a limitation may result from the principle of sovereign equality of States which is defined in Art. 2(1) of the UN Charter, and by the “principle of non-intervention”, a norm of international custom¹⁵⁴². The principle of non-intervention prohibits States from intervening coercively in the internal or external affairs of other States, the so-called “*domaine réservé*” of States.¹⁵⁴³ International organizations such as the UN can also violate this principle in relation to their Member States, Art. 2(7) of the UN Charter. A violation of this principle results in the interference with the right of self-determination of another sovereign State. This right consists of the power to freely choose its political, social, economic and cultural system and to develop its own State identity by determining the rights and obligations of citizens within its legal order. Foreign States affected by such interferences are allowed to prevent encroachments on their territory. A State has therefore the right not to recognize acts of other States and not to enforce them on its territory. To achieve such

¹⁵⁴⁰ *Weltimmo* case. // *Google Spain* case. // *Verein für Konsumenteninformation* case. // Facebook fanpages case.

¹⁵⁴¹ Herdegen, M. [Matthias]. (2020). *Internationales Wirtschaftsrecht*. C.H. Beck. § 3, paras. 69 ff.

¹⁵⁴² “The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law”. ICJ. *Nicaragua v. United States of America*, Judgment of 27 June 1986, (27 June 1986). Para. 202

¹⁵⁴³ “No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of another State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.” UN, General Assembly. *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, Resolution 2625, (24 October 1970).

enforcement, MLATs could for example be concluded, which, based on reciprocity, could regulate, inter alia, the enforcement of foreign court judgments.

A production order for personal data located outside US territory is permissible by a FISA order or a NSL if the addressee has the *de facto* ability to access these data. The application of the principle of personality allows these orders to be issued to companies that are headquartered outside the US, if the access is through a company with which the addressee of the order is affiliated through the group structure. Such orders can be in conflict with essential guarantees of the European framework. While the Cloud Act makes a data controller's legal remedies dependent on a foreign State not extending the effect of its national laws into the US, Art. 48 of the GDPR permits extraterritorial orders of a foreign State to produce personal data only under existing international agreements (especially MLATs) with the EU. Thus, both regulations reflect the attitude of granting a country's own laws the broadest possible territorial reach. This generates pressure on countries to adapt to the fact that there is a threat of restrictions on economic trade if these countries do not make concessions. Ultimately, if a country with a high level of data protection, such as the EU, decides to enter into an agreement with the US under the Cloud Act, it may in turn seek assurances of mutual legal assistance in enforcing its own laws. Otherwise, this country could give up part of its level of data protection.

Just like the establishment principle (Art. 4(1) Directive 95/46 and Art. 3(1) GDPR) and the interpretation of the *lex loci solutionis* (CJEU), Art. 3 PIPL applies not only to the processing of personal data within China, but also to data processing activities outside China, if the purpose of such processing is the provision of products and services to natural persons in China, or the analysis or evaluation of the behavior of natural persons in China. But – unlike the GDPR – it also includes “other circumstances stipulated by laws and administrative regulations”. Extraterritoriality under China's law “can therefore be expanded by other laws or regulations”¹⁵⁴⁴. Responsibilities for the processing must designate representatives within the PRC and advise their identity to the relevant supervisory authorities, Art. 53 PIPL.

Disputes over the legality of extraterritorial sovereign acts are on the rise. As a reaction to this, a defensive attitude by enacting so-called “blocking statutes” can be observed at global level. In addition to legal acts expressly designated as such, blocking statutes can also be found in substantive law, usually characterized either by non-recognition of foreign court orders or by an order to domestic legal entities to prioritize compliance with their own law, with the overall aim to prevent enforcement and thus effectiveness of foreign legislation. Blocking statutes could increase in the form of “extraterritoriality shields”¹⁵⁴⁵ against extraterritorial application of foreign data protection legislation. In so far as blocking statutes seek to achieve prioritization of domestic law outside the national territory, they themselves have an extraterritorial effect. However, this effect does not mean that a State's own sovereign act is performed on a foreign territory, but it is merely a matter of achieving consideration of its domestic law abroad.

One example comes from China, which was introduced by the “MOFCOM Order No. 1 of 2021 on Rules on Counteracting Unjustified Extraterritorial Application of Foreign Legislation and Other Measures” (MOFCOM Order 1/2021)¹⁵⁴⁶. MOFCOM Order 1/2021 can be seen as one action of Chinese government's countermeasures against the US,

¹⁵⁴⁴ Greenleaf, G. [Graham]. (1 October 2021). China's Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report*, 2021(172), <https://ssrn.com/abstract=3989775>. P. 3.

¹⁵⁴⁵ Svantesson, D. J. B. [Dan Jerker B.]. (22 January 2021). *How will China's new 'extraterritoriality shield' affect the Internet?*. <https://www.linkedin.com/pulse/how-chinas-new-extraterritoriality-shield-affect-svantesson/?trackingId=JDCdj1zwQISubFg616JUHA%3D%3D>.

¹⁵⁴⁶ Ministry of Commerce of the People's Republic of China. *MOFCOM Order No. 1 of 2021 on Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures*, <http://english.mofcom.gov.cn/article/policyrelease/announcement/202101/20210103029708.shtml>, (9 January 2021).

because the US had imposed trade sanctions and export restrictions on Chinese enterprises (e.g., through Executive Order 13959¹⁵⁴⁷), which imposed sanctions on several Chinese companies, (including HUAWEI), as also Art. 1 MOFCOM Order 1/2021 suggests. Apart from trade policy reasons, MOFCOM Order 1/2021 has also an impact on data protection regulations outside China mainland. PIPL is intended to extend the application of Chinese law abroad. MOFCOM Order 1/2021 complements PIPL in this way, as Art. 2 MOFCOM Order 1/2021 states:

These rules apply to situations where the extraterritorial application of foreign legislation and other measures, in violation of international law and the basic principles of international relations, unjustifiably prohibits or restricts the citizens, legal persons or other organizations of China from engaging in normal economic, trade and related activities with a third State (or region) or its citizens, legal persons or other organizations.

It seems therefore to be an emerging governmental reaction to expand extraterritorial claims as means on the way to a type of data protection regulation that is as advantageous as possible for the own country, as Svantesson also noted: “If extraterritoriality is a sword, it is no surprise that the increasing use of that sword is being met by shields such as that of Rules on Counteracting Unjustified Extraterritorial Application of Foreign Legislation and Other Measures”.¹⁵⁴⁸ Such “unjustified” extraterritorial application of foreign laws and other measures would exist if there is a violation of international law. This is a high hurdle, but because “international law’s regulation of extraterritoriality is largely a gray zone”, a China-friendly interpretation of Art. 2 MOFCOM Order 1/2021 is to be expected to block undesirable foreign instruments.¹⁵⁴⁹

Blocking statutes are also known in the European framework. The Council Regulation (EC) No 2271/96 expressly seeks to block what is regarded as the extraterritorial impact of some US sanctions on Iran, Libya and Cuba.¹⁵⁵⁰ The GDPR does not expressly seek to block and Naef annotated “that the EU fundamental rights-based regulation of data transfers can be justifiably considered as data protection without data protectionism”¹⁵⁵¹. Nevertheless, the GDPR may constitute a legal impediment to comply with orders of US courts. It is therefore necessary to address the interpretations of foreign courts as to whether they regard the GDPR as a blocking statute; because of the importance of the EU-US arena¹⁵⁵², especially those of the US jurisprudence). In the absence of supreme court rulings, it is still unsettled in the US whether the GDPR is a blocking statute from the US perspective – especially in e-discovery cases. According to Spies, some rulings by US district courts on data protection laws in Europe suggest the classification as a

¹⁵⁴⁷ USA, The White House. *Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies*, Executive Order 13959 of 12 November 2020, <https://www.federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies>, (17 November 2020).

¹⁵⁴⁸ Svantesson, D. J. B. [Dan Jerker B.]. (22 January 2021). *How will China’s new ‘extraterritoriality shield’ affect the Internet?*. <https://www.linkedin.com/pulse/how-chinas-new-extraterritoriality-shield-affect-svantesson/?trackingId=JDCdj1zwQISubFg616JUHA%3D%3D>.

¹⁵⁴⁹ Svantesson, D. J. B. [Dan Jerker B.]. (22 January 2021). *How will China’s new ‘extraterritoriality shield’ affect the Internet?*. <https://www.linkedin.com/pulse/how-chinas-new-extraterritoriality-shield-affect-svantesson/?trackingId=JDCdj1zwQISubFg616JUHA%3D%3D>.

¹⁵⁵⁰ “The purpose of the Blocking Statute is to counteract the extra-territorial application of laws, regulations, and other legislative instruments of non-EU countries that purport to regulate activities of natural and legal persons under the jurisdiction of the Member States.” European Commission. *Report from the Commission to the European Parliament and the Council relating to Article 7(a) of Council Regulation (EC) No 2271/96 (‘Blocking Statute’)*, COM(2021) 535 final, (3 September 2021). P. 1

¹⁵⁵¹ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 427.

¹⁵⁵² See also below Chapter IX, Section II.1.

blocking statute.¹⁵⁵³ Others argue that “while some US judges have shown sympathy towards attempts to limit discovery when it conflicts with non-US laws, they have largely rejected a party’s reliance on overseas data privacy regulations to avoid discovery altogether”¹⁵⁵⁴. Because of this uncertainty, according to Spies, the

decision in *Morgan Art Foundation Ltd. v. McKenzie, American Image Art et al*¹⁵⁵⁵ joins the chain of US decisions in which judges try to avoid settling as much as possible. Judges mostly seek to avoid conflicts of law and to reconcile the different requirements of the US and EU jurisdictions. If a party wants to invoke the limitations of Chapter V of the GDPR in US litigation or before a US authority, much depends on how it brings the GDPR into the litigation, what documents it offers, and how important the documents are in Europe. A total blockade at the e-discovery with reference to data protection usually does nothing. Otherwise, it can happen that even if a German expert appears in the US proceedings, the judge makes the ruling based on his own free interpretation of the legal text of the GDPR. The danger cannot be dismissed that a US judge will erroneously conclude based on Art. 49(1)(e) GDPR that US discovery is in any case in compliance with the GDPR.¹⁵⁵⁶

Without an “international agreement” stipulated by Art. 48 GDPR, the US Cloud Act could even be interpreted as an obligation to violate foreign law such as the GDPR. Even if the EU would sign an executive agreement with the US (which does not require parliamentary ratification in the US) and became a “qualified foreign government”¹⁵⁵⁷ under the US Cloud Act, it would still be questionable whether the procedure would meet the Art. 48 GDPR requirements. The requirements for such an agreement are compliance with procedural and legal principles as well as data protection principles, but do not specify the basis of legitimacy for a transfer of personal data to the US. In addition, the legal purpose of Art. 48 must be considered. Considering the NSA affair, the purpose was to make TFPD at the request of a third country more transparent. If we would interpret such an executive agreement as an “international agreement” within the meaning of Art. 48 GDPR, this would run counter to the purpose of the GDPR.

Furthermore, it is necessary to ask how the reaction (blocking statute) to a foreign law (e.g., US Cloud Act) can in turn be encountered with another reaction. Of interest in this regard is the decision in *Société Nationale Industrielle Aérospatiale v. U. S. Dis. Ct. for S. Dist. of Iowa*¹⁵⁵⁸. The court held that “a blocking statute does not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute. [...] American courts are not required to adhere blindly to the directives of such a statute.” This indicates that blocking statutes cannot restrict the jurisdiction of US courts. The US courts can, however, voluntarily consider impeding regulatory conflicts in the context of a “comity analysis”¹⁵⁵⁹. It is then to be determined on a case-by-case basis, whether a production of the personal data can be ordered.¹⁵⁶⁰ This production does not necessarily lead to contradicting

¹⁵⁵³ Spies, A. [Axel]. (September 2019). *US-District Court: Ist die DS-GVO ein Blockadegesetz (Blocking Statute)?*. <https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2019/us-district-court-is-the-gdpr-a-blocking-statute.pdf>. P. 3.

¹⁵⁵⁴ Potratz Metcalf, C. [Caitlin] and Lurie, A. [Adam] and Davison, D. [Doug]. (29 January 2020). *GDPR vs US Discovery: US Court Makes Clear Non-US Entities Can't Avoid Discovery*.

<https://www.linklaters.com/en/insights/blogs/digilinks/2020/january/gdpr-vs-us-discovery>.

¹⁵⁵⁵ USA. *Morgan Art Foundation Ltd. v. McKenzie, American Image Art et al*, District Court of Southern District of New York, 18 Civ. 4438 (AT), (15 December 2021).

¹⁵⁵⁶ Spies, A. [Axel]. (September 2019). *US-District Court: Ist die DS-GVO ein Blockadegesetz (Blocking Statute)?*. <https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2019/us-district-court-is-the-gdpr-a-blocking-statute.pdf>. P. 4.

¹⁵⁵⁷ See Chapter III, Section II.1.2.7.

¹⁵⁵⁸ USA. *Société Nationale Aérospatiale v. US District Court*, 482 U.S. 522, (1987)

¹⁵⁵⁹ USA. *Société Nationale Aérospatiale v. US District Court*, 482 U.S. 522, (1987). P. 544 ff.

¹⁵⁶⁰ USA. *Richmark Corp. v. Timber Falling*, 959 F. 2d 146, 9th Cir., (1992). P. 1475.

obligations of the service provider. For example, the US Department of Justice recognized that there are blocking statutes that can prevent a company from following a court order and applies requirements to records containing personal data abroad: “Where a company claims that disclosure of overseas documents is prohibited due to data privacy, blocking statutes, or other reasons related to foreign law, the company bears the burden of establishing the prohibition. Moreover, a company should work diligently to identify all available legal bases to provide such documents”.¹⁵⁶¹

Consistent application of blocking statutes may contribute to a decline in extraterritorial laws in the long run, as this application might prevent enforcement and thus the effectiveness of the foreign law. But this can lead to legal uncertainty. Moreover, since the EU and the US are not pursuing joint conflict resolution in this regard, obligated companies continue to find themselves in a dilemma, especially the CSPs. Whole server farms were set up on a territory without any or only limited protection of personal data. This ultimately revitalized the problem of “forum shopping”¹⁵⁶².

Those responsible for a TFPD which are also subject to European law can be confronted with three possible reactions whenever their production of personal data has been requested from the US side. First, a complete avoidance of the production of personal data, which is only possible, if at all, if no personal data were transferred to companies that potentially fall within the scope of US law, by fulfilling these action items:

- The EU-based subsidiary has all its offices in the related EU country, conducts no business in the US, and operates independently of its corporate parent in the US; and
- the computer network established in the EU-based subsidiary is fully segmented from the network of its corporate parent; and
- as a technical matter, it is not possible for personnel of the corporate parent to reach remotely into the telecommunication infrastructure of the EU affiliate to obtain data.¹⁵⁶³

If this is not feasible, it may be advisable to contract with EU-based companies only, or to enact so-called “silo solutions”, by seeking

to modify the service provider agreements to limit U.S. access to the data held in non-U.S. jurisdictions, including in the European Union. As part of such a risk mitigation, agreements with U.S. service providers should be evaluated to determine whether data held outside of the U.S. by non-U.S. legal entities is accessible via keyboards in the U.S. Language should be added to such service provider agreements to make clear that non-U.S. data are “siloed” (physically and logically segregated) at non-U.S. data storage locations and cannot be accessed from the U.S. Further, unless such notification is prohibited by law, prospective service recipients that envisage entering into service agreements with these types of service providers should seek to use contractual language committing the U.S. service provider to notify them, as service recipients, of having received a legally binding request under the CLOUD Act.¹⁵⁶⁴

Second, the company in question could transfer personal data to its US-based corporate parent and only then produce personal data within the US to the respective US authority. The first inner-corporate transfer would then take place within the scenario of a TFPD to a third country. This option would not affect the scope of Art. 2(2) GDPR, because the

¹⁵⁶¹ USA, Department of Justice. *Justice Manual*, 9-47.120 - FCPA Corporate Enforcement Policy, § 9-47.120, <https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977>, (2022).

¹⁵⁶² See also Chapter II, Section II.3.1.

¹⁵⁶³ Artzt, M. [Matthias] and Delacruz, W. [Walter]. (29 January 2019). *How to comply with both the GDPR and the CLOUD Act*. <https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act>.

¹⁵⁶⁴ Artzt, M. [Matthias] and Delacruz, W. [Walter]. (29 January 2019). *How to comply with both the GDPR and the CLOUD Act*. <https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act>.

transfer would initially be conducted between two controllers and would therefore not directly serve for national security rationales or similar. The third option is such of a direct data transfer from companies outside the US to US authorities. If personal data leave a foreign jurisdiction (e.g., the EU), the risk situation escalates and fundamental rights (e.g., from the Charter) cannot guarantee effective protection of the data subjects.

CSPs therefore reacted and started offering options for processing personal data exclusively on servers within Europe. Microsoft Ireland Ltd., e.g., had given their European B2B customers the opportunity to use SDPC. With the “German Cloud”, Microsoft and T-Systems promised their German customers full control and decision-making sovereignty over their personal data and, ultimately, remedial measures against access by US. Within this new structure, using only German T-Systems’ data centers, access rights are only granted for a limited period in individual cases and the data processing is carried out by a so-called “data trustee”, not Microsoft itself. Access to personal data is, if necessary, recorded in a logbook, to which Microsoft has no access. Politicians also reacted by promoting a “European Cloud”. The German Gaia-X project, e.g., is “a next-generation, decentralized, federated data infrastructure”, but will “not be a stand-alone cloud solution in the classic sense. The German government has no intention of developing a European cloud provider”.¹⁵⁶⁵ Nevertheless, the “European Cloud” became a strong selling argument for various CSPs in Europe. Another regulatory piece, which is moving in a similar strategic direction, is the draft EUCS¹⁵⁶⁶. It “includes sovereignty requirements on European data localization and foreign law immunity, [...] would mirror requirements recently introduced in France’s national cybersecurity certification scheme, known as SecNumCloud, and would affect cloud service providers operating in the EU market, ensuring that EU law is primary and that maintenance, operations and data must be located within the EU.”¹⁵⁶⁷

The GDPR claims application beyond the borders of the EU, especially through Art. 3(2) GDPR, but on the other hand is not able to fulfill its global claim through effective enforcement. Kloth noted that it is “exactly this gap between promise and delivery that could undermine the legitimacy of the GDPR’s extraterritorial applicability. Applicability and enforceability are two sides of the same coin. Therefore, it appears to be inconsistent to adopt a law, which may be applied extraterritorially but cannot be effectively enforced in the same way”¹⁵⁶⁸. Svantesson therefore classified this approach as “bark jurisdiction”, opposed to a real attempt by a “bite jurisdiction”, and explained why States nevertheless want to establish the international legitimacy of their attempts to protect the personal data of their citizens: “First, there is the mentioned symbolic value in showing an attempt at treating domestic and foreign organizations equally. And second, the claim of an extraterritorial effect may have a deterrent effect, at least if we assume that companies generally prefer not to violate any laws”¹⁵⁶⁹. This shows that especially for MNEs, the event of a conflict of laws is a problem driver, which may lead to legal uncertainty. In a global and interdependent economy, companies and data subjects need such certainty, especially about data as the core of the digital transformation of the economy in the 21st century. It should therefore be clear which State institutions have access to data at home and abroad, in which cases, and on which legal basis. If this problem remains

¹⁵⁶⁵ Deutscher Bundestag. *Antwort der Bundesregierung*, Drucksache 19/21077, (14 July 2020). P. 4

¹⁵⁶⁶ See also Chapter II, Section II.3.8.2.

¹⁵⁶⁷ Kabelka, L. [Laura]. (16 June 2022). *Sovereignty requirements remain in cloud certification scheme despite backlash*. <https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash>.

¹⁵⁶⁸ Kloth, A. [Alexander]. (5 February 2018). *One law to rule them all, On the extraterritorial applicability of the new EU General Data Protection Regulation*. <https://voelkerrechtsblog.org/de/one-law-to-rule-them-all>.

¹⁵⁶⁹ Svantesson, D. J. B. [Dan Jerker B.]. (2015). Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*, 5(4), 226–234. P. 233.

unaddressed it could, especially in the US-EU arena, continuously affect trust of end-users, as the following statistic highlights.

Data protection concerns against American providers of online offerings until 2018:¹⁵⁷⁰ Percentage of respondents who are concerned about storing their personal data with American companies in Germany from 2010 to 2018.

2010	64,7	in %
2011	67,8	in %
2012	68,9	in %
2013	73,8	in %
2014	73,4	in %
2015	72,5	in %
2017	72,5	in %
2018	76,5	in %

Legislation with extraterritorial reach considered in this Section III may also run counter to security interests. There could be an erosion of international security cooperation, on which many States continue to rely because of transborder threat situations. Furthermore, there is the threat of the so-called “reciprocity objection”. If, for example, European law enforcement can demand that SPs operating in the European internal market produce personal data (even if these are located abroad or process personal data of foreigners), the objection seems reasonable that agencies such as from the US should be able to do the same reciprocally and demand SPs to produce personal data located on European servers or concerning European citizens. The comment by John Frank, vice president for EU government affairs at Microsoft, could then eventually come true: “If every country asserts extraterritorial jurisdiction [...] then everybody gets everybody’s data.”¹⁵⁷¹ This in turn could threaten the “gold standard” of the GDPR proclaimed by the EU, lead to businesses enacting “silo solutions”, and data subjects resorting to encryption techniques, both not necessarily helpful for effective law enforcement measures.

IV. Conclusive remarks

As explained, TFPD raise a considerable number of “problem drivers”. Problem drivers lead to consequences categorized in three problem categories under which the “core problem” falls. This core problem – which is the dilemma of a free flow of personal data vs. restrictions on the free flow of personal data – can be linked to several problem drivers. In practice, “a country’s regulatory framework on cross-border data flows can be based on policy rationales falling under overlapping lenses”. Problem drivers are therefore not always clearly separable from each other because there may be even hidden rationales in regulatory measures. Once these rationales are unjustified, they usually become a problem driver.

Thereby exist relatively clearly recognizable drivers, which arise from unjustified rationales; such were determined in Section I.1. to Section I.3. of this Chapter VIII as those balancing the interests of data protection and data flow restrictions for (i) national security, (ii), public order (judicial investigations), and (iii), ensuring a national digital economy policy. Sections II and III of this Chapter VIII determined drivers that can be

¹⁵⁷⁰ Statista GmbH. (5 May 2023). *Anteil der Befragten, die Bedenken haben, ihr privaten Daten bei amerikanischen Unternehmen zu speichern, in Deutschland in den Jahren 2010 bis 2018*. <https://de-statista-com.ezproxy.ip.mpg.de:8443/statistik/daten/studie/869457/umfrage/datenschutzbedenken-gegenueber-amerikanischen-anbietern-von-online-angeboten-in-deutschland>.

¹⁵⁷¹ Julia Fioretti, J. [Julia]. (26 February 2018). Europe seeks power to seize overseas data in challenge to tech giants. *Reuters*. <https://www.reuters.com/article/uk-eu-data-order-idUKKCN1GAOLN>.

counted as falling under data sovereignty, but which can concern measures other than solely data flow restrictions.

The goal of a free flow of personal data is manifested in all relevant regulatory instruments discussed in this thesis. At the same time, however, there is a trend towards more protectionism. A G20 policy brief, which discussed how “deglobalization” affects the role and relevance of international trade institutions and agreements, noted approvingly that “the period ahead may be characterized by further trade tensions, magnifying the danger of deglobalization”¹⁵⁷².

This protectionism consists of limiting TFPD out of a wide variety of rationales, which overlap. A precise delimitation of these rationales is difficult, but not impossible. On the one hand, there is the rationale of national security in the broad sense, which includes safeguarding defense interests, public security, or – more vaguely – important objectives of general public interest. Law enforcement forms a second rationale. These two rationales are explicitly standardized in some of the regulatory measures examined. However, these rationales are not always as directly mentioned as in the EU Single Market Strategy. The latter, like other supranational frameworks of this kind, still suffers from the fact that “a real market [...] on data storage is yet to come into function in practice: Two-thirds of all demand for ICT-related services (consulting, hosting, development) are sourced locally within each Member State, while only 18% is sourced from the rest of the EU. Meanwhile, the cost difference of operating data centers can be considerable amongst the EU Member States, with the most expensive country being twice as expensive as the cheapest”¹⁵⁷³. This can lead to a focus on the development of this market through regulatory measures, including protective ones against all those outside this market to reduce the complexity of the matter. The analysis of these measures and their rationales is made more difficult when, as happens, considerations relating to the protection of the national digital economy are framed in a codified way. Exemplarily, the rationale of preventing circumvention of a State’s own law plays a role in basically all the rationales mentioned in Section I; Kuner also noted that this rationale “applies both to territorial scope rules and data transfer restrictions”¹⁵⁷⁴.

Section I found that data flow restrictions do not achieve the objectives that follow from the rationales. On the contrary, they lead to demonstrably negative effects. Cory / Dascoli concluded that

restricting data flows has a statistically significant impact on a nation’s economy – sharply reducing its total volume of trade, lowering its productivity, and increasing prices for downstream industries that increasingly rely on data. Using a scale based on OECD market-regulation data, [the Information Technology & Innovation Foundation] ITIF found that a 1-point increase in a nation’s data restrictiveness cuts its gross trade output 7 percent, slows its productivity 2.9 percent, and hikes downstream prices 1.5 percent over five years.¹⁵⁷⁵

An ECIPE policy brief found that “the economic loss generated by full data localization by each of the Member States would lead to a loss of EU-wide output by 52 billion euros

¹⁵⁷² Sait Akman, M. [Mehmet] et al. (7 October 2021). *Confronting Deglobalization in the Multilateral Trading System*. https://www.t20italy.org/wp-content/uploads/2021/09/TF3_PB02_LM04.pdf. P. 4.

¹⁵⁷³ Bauer, M. [Matthias] and Ferracane, M. [Martina] and Lee-Makiyama, H. [Hosuk] and van der Marel, E. [Erik]. (December 2016). *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localization Measures in the EU Member States*. <https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu>. P. 1.

¹⁵⁷⁴ Kuner, C. [Christopher]. (16 April 2021). *Territorial Scope and Data Transfer Rules in the GDPR: Realizing the EU’s Ambition of Borderless Data Protection*. *University of Cambridge Faculty of Law Research Paper No. 20/2021*, <http://dx.doi.org/10.2139/ssrn.3827850>. P. 9.

¹⁵⁷⁵ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

per year (0.37% of GDP). This number will increase with further digitalization of the European economy"¹⁵⁷⁶. Ustaran found that

data localization is a myth. Information is global. Communications are global. The internet is global. So data localization in the sense of geographically ring-fencing data to make it inaccessible from other parts of the world is simply inviable. [Nevertheless] different organizations have responded [to data localization] in different ways, but essentially, even the most global of organizations have had to strengthen their relationships with local businesses to demonstrate that globalization is not in conflict with local partnerships and the employment of workforces on the ground. This is likely to become a growing pattern that will test the true global credentials of many businesses seeking to operate across borders.¹⁵⁷⁷

UNCTAD found that

as long as there is not a properly functioning international system of regulations for cross-border data flows to ensure maximization of the value of data, private and public, while protecting them from harm, and equitably distributing those gains within and between countries, there will be no alternative for countries to ensure that the domestic economy benefits from the development gains from the data, other than trying to keep their data inside national borders. However, it is important to consider that, while on the one hand there cannot be value without the raw data, on the other hand, having access to the data without the capacity to process and monetize them, or to create social value, is of no use. In this context, imposing restrictions for cross-border data flows may lead to no benefits, while creating barriers and uncertainty for firms and individuals seeking to exchange data across borders.¹⁵⁷⁸

Such restrictions do not only lead to negative effects for national economies as such, but also for the microeconomy, namely for MNEs. Those are often active in many countries as part of their business activities and rely on TFPD. The WTO found that "regulatory conditions or requirements on transferring data, and data localization policies, i.e., regulatory requirements to store or process data locally, can force exporters to build or lease data centers in every country of operation. Doing so can impose prohibitively high compliance and entry costs"¹⁵⁷⁹.

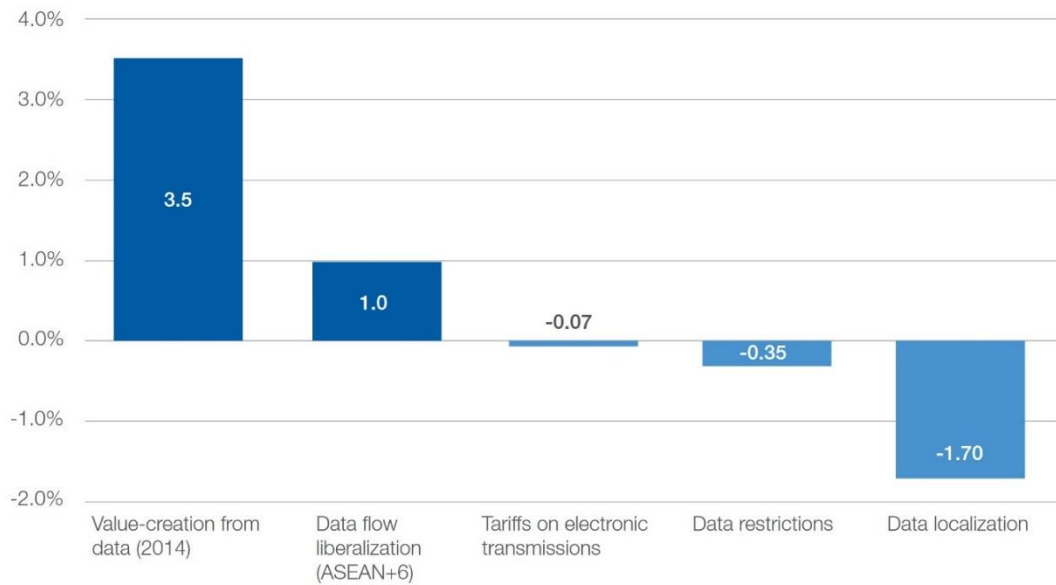
¹⁵⁷⁶ Bauer, M. [Matthias] and Ferracane, M. [Martina] and Lee-Makiyama, H. [Hosuk] and van der Marel, E. [Erik]. (December 2016). *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localization Measures in the EU Member States*. <https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu>. P. 1.

¹⁵⁷⁷ Ustaran, E. [Eduardo]. (16 June 2022). *In search of a data localization strategy*. <https://www.linkedin.com/pulse/search-data-localization-strategy-eduardo-ustaran>.

¹⁵⁷⁸ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 93.

¹⁵⁷⁹ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 9.



Source: World Economic Forum, “The cost of data restrictions”¹⁵⁸⁰

MNEs are also faced with various legal systems that determine the applicability of data protection regulations differently and at the same time place divergent requirements on data protection concepts (Section II). MNEs that must comply with the GDPR tend to adopt the stringent European regulations for reasons of simplicity, and to maintain them even in such countries whose laws are less stringent. Some argue that Europe holds a worldwide pioneer position in data protection policy. The more foreign MNEs are voluntarily oriented to the level of protection set by the GDPR, the more the GDPR could resemble a global gold standard. But such standard should in any case not hinder a right balance between national interests and those of international trade, as Cécile Barayre also noted: “Ensuring that laws consider the global nature and scope of their application, and foster compatibility with other frameworks, is of importance for global trade. Getting the balance wrong between data protection and data flows can have serious consequences for either the protection of fundamental rights or for international trade and development.”¹⁵⁸¹

This balance is also complicated by another problem driver, which is the exercise of extraterritorial jurisdiction, discussed in Section III. Regulations with extraterritorial reach represent a problem of delimitation of jurisdiction between sovereign States, as they affect interests of other States. A regulation is extraterritorial if it exercises sovereignty in such a way that people, objects, or actions outside a States’ own territory are also subject to domestic law. Such regulation is only permissible if the subject-matter of this regulation has a significant connection with the domestic market. This evidence is provided based on accepted connecting factors. These connecting factors illustrate that regulations with extraterritorial reach are in principle made for reasons of protecting own citizens or market regulation, but they are also used to pursue data protection and economic interests. Since WTO law guarantees a right to market access under international law, such enforcement of a State’s own data protection provisions may be justified, provided that it complies with the requirement of proportionality. A balancing of interests is therefore required before exercising a States’ sovereignty. In determining this

¹⁵⁸⁰ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 9.

¹⁵⁸¹ Barayre, C. [Cécile]. (5 July 2016). *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. MIKTA Workshop on Electronic Commerce, Geneva, Switzerland.

https://www.wto.org/english/forums_e/business_e/3_4_Cecile_ppt.pdf. P. 6.

proportionality, it is then also necessary to consider that a MNE can have both feet on the ground in different jurisdictions. The search for a proportionate balance between the right to market access and the requirements of data protection indirectly becomes then the place for establishing practical concordance between competing jurisdictions in TFPD scenarios.¹⁵⁸² The extraterritorial claim to regulate data protection is nevertheless not abandoned, despite the associated problems, but is considered necessary, so that new laws with extraterritorial scope are still frequently passed. Nevertheless, excessive use of sovereignty constitutes a jurisdictional overreach, which can lead to a violation of the principle of non-intervention. In its worst form, such types of regulatory measures can lead to blocking statutes and lock-in effects.

The exercise of extraterritorial sovereignty depends on the particularities of the respective jurisdiction. We addressed therefore the nature and scope of the right to data protection as another problem driver in Section II of this Chapter. As noted, there are differences in the understanding of this right. There are arguments “that non-personal (and industrial) data is a critical input to the industry and involves less divisive policy issues, making a multilateral consensus more likely. Yet, the cross-border flow of non-personal data still depends on the granular details that govern the local definition of personal data since it is defined negatively, *e contrario*, as any data that is not personal information”¹⁵⁸³. This in turn causes uncertainty among legislators and ultimately leads to a tendency to a jurisdictional overreach.

This is reinforced by the fact that some new regulatory measures hold considerable ambiguity about the details of extraterritorial application. In China’s PIPL, for example, “data transfer agreement” is not yet specified, reliance on CAC decisions in Art. 38 PIPL is vaguely extended to “other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department”, Art. 13(6) PIPL is significantly vaguer than the GDPR in that it does not specify what types of laws and administrative regulations may create such a ground for data processing, and Art. 41 PIPL leaves undefined who qualifies as a foreign “judicial or law enforcement” agency, and who as the competent Chinese authority to grant approval.

Transfer mechanisms therefore remain essential to avoid data localization.¹⁵⁸⁴ To avoid conflicts of interests, some attempts have been made to compensate for them through bilateral agreements, in some cases the conflict was even deliberately accepted. Nevertheless, the problem of which issues should be addressed by international agreements remains an open issue at stake. This endangers “the potential for an open, rules-based, and innovative global digital economy. Data localization makes the Internet less accessible and secure, more costly and complicated, and less innovative”¹⁵⁸⁵. There is therefore a potential threat to the universality of the international legal system regarding TFPD. The technology gap, although decreasing year by year between developed and developing States due to a technological globalization, could, untreated, result in a regulatory split.

¹⁵⁸² Von Arnould, A. [Andreas]. (2016). Freiheit und Regulierung in der Cyberwelt: Transnationaler Schutz der Privatsphäre aus Sicht des Völkerrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 1–34). C.F. Müller Verlag, P. 22.

¹⁵⁸³ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 16.

¹⁵⁸⁴ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 17.

¹⁵⁸⁵ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

At the end of this process could stand an international law no-harm rule shaped by fundamental rights protection, if a worldwide largely uniform level of data protection could be reached. Such level is expected from those concerned to ensure that personal data are adequately protected in a world shaped by the Internet. At the same time, such level should enable companies to adopt a uniform data protection concept. These “similarities” mentioned by the WEF are to be examined in the following Chapter IX.

CHAPTER IX: THE GLOBAL ECOSYSTEM OF TRANSBORDER FLOWS OF PERSONAL DATA

The aforementioned¹⁵⁸⁶ specific methodology places emphasis on the evaluation of stakeholder interests. The (core) problem defined in Chapter VIII “emerge between different policy objectives at the national level, and between countries, as well as different interests among various actors in relation to cross-border data flows”¹⁵⁸⁷ and therefore represent the link between Chapter VIII and Chapter IX. These problems can at the same time provide an impetus for legislation. This impetus is dependent on an estimation of potential disruptive events and the associated probability of negative regulatory impacts. This estimation begins in the present Chapter IX and continues in Chapters X and XI.

This Chapter will incorporate the aforementioned¹⁵⁸⁸ multi-stakeholder approach. It will therefore present views of the stakeholders involved, because due to the tension in this thesis between the “dimensions” described above¹⁵⁸⁹, a legislator should carry out an open, transparent, and interdisciplinary procedure. This approach should address the

complexity of relations among different actors in the digital economy at national and international levels. The lines between countries and actors represent the different tensions that may emerge. Discussions on cross-border data flows highlight that rulemaking emerges in context-dependent ways in terms of different data categories and data flows, based upon different perspectives [...] Policymaking in this area requires recognizing the complexity of the conflicting interests, dilemmas and trade-offs that arise, and properly assessing them. This implies policy choices, as interests may go in different directions. Policymakers will therefore need to assign weights to the different interests and objectives, and find the necessary balance that meets their specific needs and supports their development objectives.¹⁵⁹⁰

The UN had already stated in 2006 that “there are restrictions and exceptions and competing interests recognized in the protection of informational data. Indeed, the privacy protections offered by national Constitutions and in judicial decisions and international human rights instruments recognize possible restrictions and exceptions, in

¹⁵⁸⁶ Chapter I, Section II.4.

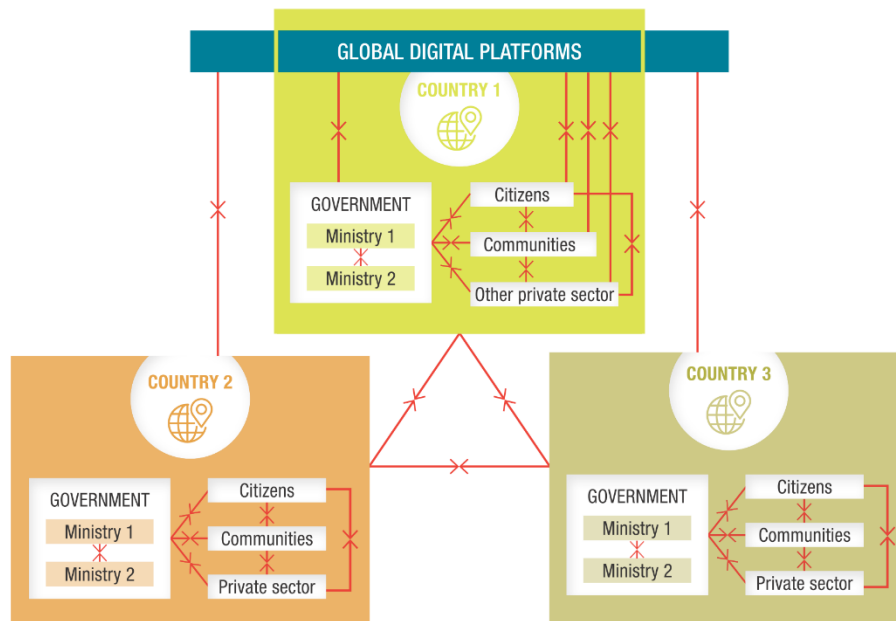
¹⁵⁸⁷ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 89.

¹⁵⁸⁸ Chapter I, Section II.4

¹⁵⁸⁹ Chapter I, Section I.

¹⁵⁹⁰ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 89. // Similarly in Trakman, L. [Leon] and Walters, R. [Robert] and Zeller, B. [Bruno]. (2019). Is Privacy and Personal Data Set to Become the New Intellectual Property?. *International Review of Intellectual Property and Competition Law*, 937–970, <http://dx.doi.org/10.2139/ssrn.3448959>. P. 964–965: “It is also potentially treacherous in recognizing the competing personal and commercial interests involved, and limitations in reconciling disparate regulatory measures. [...] It is our view that, given the divergence between these legal systems, the pathway forward would entail greater legal convergence around key concepts and principles, such as in the definition of personal data and in consent to collecting, processing and other use of that data. This approach has, arguably, been successful in other areas of private international law, such as in international trade law. However, the challenge for policy makers in the field of data protection lies in the multi-layered approach and direction that data protection laws have assumed to date.”

the form of derogations or limitations.”¹⁵⁹¹ The types of stakeholders therefore result in different interests, consequences, and interdependencies with other stakeholders.



Source: United Nations Conference on Trade and Development, “Different actors and complexity of relations in the context of cross-border data flows”¹⁵⁹²

The present Chapter IX will explain which interests a State and its organs may have in complying with its positive and negative obligations to protect its citizens in the area of data protection. This is necessary because data subjects, another stakeholder in this approach, who in their everyday lives mostly perceive conveniences and progress brought by technology, are at first hardly aware of the associated risks. Furthermore, the interests of MNEs are important because they have a responsibility to the public as well as to their corporate success.

Regulations described in Chapters II–VII are to be applied in a complex global ecosystem of transborder data flows. This ecosystem influences legislators. In the resulting “regulatory mosaic” – as shown in Chapters II–VII – the coherence of data protection as a fundamental right is difficult to guarantee, because “the threats in the consumer privacy space – absent a Snowden-equivalent privacy meltdown – are arguably less transparent and more complex, considering the vast number of stakeholders involved, the distributed nature of the relevant processes, and centrifugal forces at play”¹⁵⁹³. Other complicating factors are spontaneous, decentralized, or private legal regimes created by sometimes not even legitimized stakeholders which exercise public authority.

As considered in the hypothesis of this thesis, this ecosystem could be subject to an “international order” in this field of law. Characteristic for an international order is the relationship between power and norm, respectively between enforcement of interests and rule-boundness. To achieve such order, a balance should be found between stakeholders, each with its own interests and geopolitical position, as well as different economic resources and military forces. It should be considered that States enter the

¹⁵⁹¹ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications.

A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 20.

¹⁵⁹² UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 89.

¹⁵⁹³ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 340.

international stage as a legally embodied community with its own order and are embedded in relationships, at least with their neighbors. These relationships also find expression in bilateral or multilateral agreements that these States have already concluded in the field of data protection law. The likelihood of acceptance of an international order by such States could therefore increase if such order could provide a minimum level of participation in and protection of public goods for all associated States and if it can form a basis of stability; the latter requires mechanisms that at least provide incentives for hegemonic powers to follow the rules and counteract the abuse of superiority. POTUS Barack Obama had also recognized this danger of abuse and formulated an approach to strengthen conflict avoidance measures in his “Security Strategy 2015”.¹⁵⁹⁴

The relationship between power and norm is also found in the human mind, which combines two different systems of thought: a rational one that acts deliberately and according to plan, and an emotional one that acts quickly and smoothly. Similarly, this Chapter wants to distinguish between these two antagonistic sides. The secret to good decision-making is knowing when to rely on which of the two systems and how to balance them. This antagonism, which shapes both stakeholders and interests, will be allocated below to so-called “endogenous variables” and “exogenous variables”. This allocation or model, which originates from economics, seems appropriate, because it leads to a simplified representation of reality, which is reduced to what is necessary. For one thing, a representation of reality, which consists of a wide variety of “dimensions” (Chapter I), could be too complex and thus overwhelm a comparative law approach. On the other hand, without such a modeling, this thesis could run the risk of including too many elements, which would result in an unordered analysis, likely delving in issues not causally related to the core of the research questions. While models inescapably entail some degree of simplification, they are nevertheless important to understand contexts. This model should help to show the essence of the global ecosystem of transborder data flows and to simplify the recognition of correlations.

An exogenous variable is determined outside the model and is the input to a model. Exogenous variables are fixed the moment they are introduced into the model. These variables are the currently existing “archetypes” of data protection regulation, the “essential guarantees”, and, incorporated within both, the data protection principles. All three together represent the norm or rule-boundness. In contrast, endogenous variables are determined within the model and represent the output of a model. These variables are the stakeholders and their interests, which naturally change faster than norms. This should showcase how an intervention by one or more exogenous variables affects one or more endogenous variables. Once all variables are presented in this Chapter, it should be possible to present, in Chapters X and XI, objectives and options for a possible regulatory intervention and to theorize about their effects in practice.

At the intersection between endogenous and exogenous variables are the “arenas”, or otherwise called “games” or “use cases”. “Arenas” is inspired by the concept of the “ecology of games” described by Dutton and Peltu:

A “game” is defined [as] an arena of competition and cooperation structured by a set of rules and assumptions about how to act to achieve a particular set of objectives. Internet governance can then be seen to be the outcome of a variety of choices made by many different players involved in separate but interdependent governance games.

¹⁵⁹⁴ USA, The White House. *The 2015 National Security Strategy*, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf, (6 February 2015). P. 10-11.

This indicates that no single set of actors actually seeks to control governance as such, but that each player pursues more focused goals in collaboration or competition with other actors.¹⁵⁹⁵

Each arena contains exogenous and endogenous variables, both related to a legal issue. Assuming that the global ecosystem of transborder data flows is the totality of all possible variables, the arena “EU-US data transfers” for example would be a subset. However, only a certain number of stakeholders participate with their interests in each subset, and only certain norms are relevant for each arena. Ideally, these arenas should be delimited insofar that each arena encompasses the largest possible number of stakeholders and interests, so that both can be assigned to at least one arena to allow examining them in full. In such arenas, stakeholder interests face arising problems in the regulation of data protection. It is therefore important to keep in mind the difference between “arenas” (this Chapter IX) and “problem categories and problem drivers” (Chapter VIII). Both can, but do not necessarily have overlaps. Arenas should focus on the model of the interplay between exogenous and endogenous variables described above and have a more strategic focus, like a dispute resolution negotiation which is limited to one area of conflict.

At the end of this Chapter, it should therefore be possible to undertake a “strategic foresight” to enhance at a later point in this thesis that a proposed solution (Chapter XII) would be fit for the future. This strategic foresight

anticipates trends, risks, emerging issues, and their potential implications and opportunities in order to draw useful insights for strategic planning, policy-making and preparedness; Informs the design of new [...] initiatives and the review of existing policies in line with the revamped Commission Better Regulation toolbox; Problem categories shall then turn to the legal problems that may arise, collectively influencing all arenas.¹⁵⁹⁶

I. Endogenous variables

The starting point for the present Chapter will be to identify stakeholders and interests within the global ecosystem of transborder data flows. While these stakeholders may have interests in common, there may be conflicts in several intentions to be determined; even if those intentions are found to be in common, there are often different ideas about how, i.e., by what means, these should be achieved.

As mentioned above¹⁵⁹⁷, international law can partly still be seen not as “hard law” but merely as a collection of “noble intentions” which cannot be enforced against sovereign States. This approach cannot be followed because the international order of data protection law can to a large extent not only be seen as an intention but as “political law”, whose dependence on political structures and relations is visible. This is especially justifiable when these structures and relations change as rapidly as in the field of data protection. Prof. Hörnle also commented on this aspect and argued that “International

¹⁵⁹⁵ Dutton, W. H. [William H.] and Peltu, M. [Malcolm]. (November 2005). *The Emerging Internet Governance Mosaic: Connecting the Pieces*. <http://dx.doi.org/10.2139/ssrn.1295330>. P. 18.

¹⁵⁹⁶ European Commission. (2023). *Strategic foresight*. https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight_en.

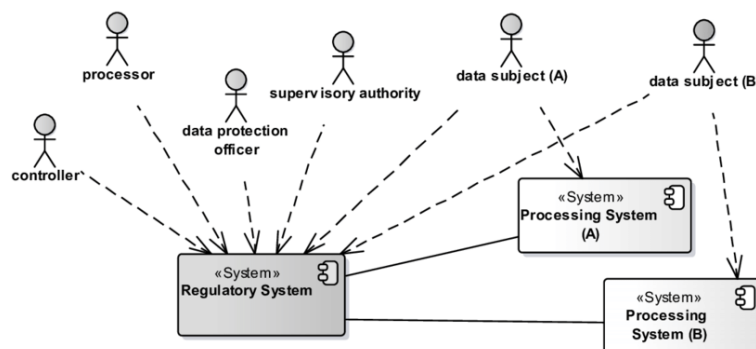
¹⁵⁹⁷ Chapter I, Section II.5.5.

law depends a lot on politics. In theory, legal frameworks are equally recognized, but always dependent on political actors”.¹⁵⁹⁸

In defining the Internet as the driver for data flows in legal terms, the boundaries between public and private law become blurred. However, the differentiation between public and private stakeholders retains its justification, primarily for the following reasons:

- As long as, and to the extent that, international law does not directly address private individuals and in particular does not recognize them as bearers of human rights obligations, this differentiation is necessary.
- Along a regulatory process, the difference between classical types of regulation (public stakeholders), pure self-regulation (private stakeholders), and co-regulation (private and public stakeholders) is important.
- Regulatory instruments distinguish in their main regulatory target field between public and private stakeholders. For instance, the GDPR (transfer private-private), the LED and the Umbrella Agreement (public-public), the Cloud Act (public-private), and the E-Evidence Regulation (public-public, but also public-private in cases of direct cooperation between a public authority and a SP or direct access to electronic evidence by a public authority).
- A data flow process oscillates between public and private stakeholders. The legislator has also recognized this and is now trying to better differentiate between the “scenarios” in a data flow; this has recently been shown by the new SDPC adopted by the Commission: the “controller-processor-set” and “third-countries-set”.

Stakeholders and their interests can best be assigned to their respective influences in two ways: first, along the stakeholders of a TFPD scenario, and second, along the stakeholders involved in a regulatory process.¹⁵⁹⁹



Source: Fernandes, M. [Mário] and Rodrigues da Silva, A. [Alberto], “Systems and stakeholders defined in the scope of GDPR”¹⁶⁰⁰

¹⁵⁹⁸ Hörnle, J. [Julia]. (2021). *Internet jurisdiction*. Oxford University Press. P. 451. // Hörnle J. [Julia]. (26 March 2021). *Roundtable - Overcoming the Jurisdictional Challenge of the Internet?*. Queen Mary University of London, Centre for Commercial Law Studies. <https://www.qmul.ac.uk/ccls/events/past-events/videos-and-recordings/overcoming-jurisdictional-challenge-of-internet/>.

¹⁵⁹⁹ Similarly differentiate Fernandes and Rodrigues da Silva: “the GDPR is an elicitation source of not only business but also system requirements to consider when developing information systems able to communicate with those that process individuals’ personal data, in order to materialize the regulatory data protection capabilities disposed in the GDPR. This may imply the existence of two types of systems: regulatory systems and processing systems, whose operation includes, yet it is not restricted to processing individuals’ personal data”. Fernandes, M. [Mário] and Rodrigues da Silva, A. [Alberto]. (2018). *Specification of Personal Data Protection Requirements: Analysis of Legal Requirements based on the GDPR Regulation*. In *Proceedings of the 20th International Conference on Enterprise Information Systems - Volume 2, ICEIS* (pp. 398–405). SciTePress. P. 400.

¹⁶⁰⁰ Fernandes, M. [Mário] and Rodrigues da Silva, A. [Alberto]. (2018). *Specification of Personal Data Protection Requirements: Analysis of Legal Requirements based on the GDPR Regulation*. In *Proceedings of the 20th International Conference on Enterprise Information Systems - Volume 2, ICEIS* (pp. 398–405). SciTePress. P. 400.

Deviating from the graphic above, we are of the opinion, as will be explained in more detail below, that although data subjects are “suppliers” of personal data and thus input to “processing systems”, data controllers, data (sub)processors, and SAs also have influences on TFPD scenarios.

1. Stakeholders of a transborder flow of personal data flow scenario

1.1. Data controllers

It is first important to distinguish which types of data controllers can participate in a TFPD scenario. Similar considerations have recently been made by the Commission when conducting RIAs concerning data flows, for example in the course of the E-Evidence Regulation.¹⁶⁰¹ Certain types of data controllers can participate in various scenarios of data flows: Public authority <-> public authority, public authority <-> private person, public authority <-> legal entity, legal entity <-> private person, legal entity <-> legal entity, private person <-> private person (unless personal data are processed for purely personal or household activities, as also Art. 2 (2) (c) GDPR excludes this scenario).

Like all other stakeholders mentioned in the present Chapter IX, data controllers are users of the Internet. They are regularly interested in a free flow of data. Apart from the interests of research companies, which focus on the exchange of scientific results, their interest in a free flow of data is identical with the economic interest in free trade. Today, the competitiveness of many companies across all sectors of the digital economy can only be ensured across resources of the Internet. The interest in a free data flow is thus a direct consequence of today’s high degree of globalization of the digital economy. The question that such data controllers therefore ask themselves is whether the lack of harmonized global data protection regulation could be opposite to their business interests.

Data controllers participate in the digital economy by using the value of personal data being processed within their business models. The latter are increasingly built on data controllers processing these data in different locations and offering their services swiftly and in line with the needs of users at different locations, especially in Big Data models. One interest of these data controllers therefore is to make regulation scalable at a global level.

Data controllers are also dependent on their home market being competitive. Hereby, diametric interests between EU-based and US-based data controllers become evident. The processing of personal data in the digital economy is largely carried out by non-European data controllers, based on a cloud infrastructure in which European CSPs have only a marginal share.¹⁶⁰² EU-based data controllers therefore have an interest in the successful implementation of the Commission’s Data Strategy¹⁶⁰³, which includes *inter alia* to promote the voluntary exchange of data, but also to focus on the underlying digital infrastructure by setting up a European Cloud. Data controllers tend to strengthen their data center capabilities and resources within the EU. This (re)location process is intended not least to provide data controllers with an assurance recommended by the

¹⁶⁰¹ European Commission. *Commission Staff Working Document, Impact Assessment, Accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118 final, (17 April 2018). P. 9–10.

¹⁶⁰² See Chapter II, Section II.3.8.2.

¹⁶⁰³ See Chapter II, Section II.3.8.2.

EDPB.¹⁶⁰⁴ The EDPB stated that remote access from a third country also constitutes third country transfers and that an agreement that the location of the data is limited to the EU is not sufficient. However, the EDPB also pointed out that merely having access from a third country does not open *Schrems II* risks, provided the provider is based in the EU and assures that no data processing takes place in third countries despite the access possibility. Whether this is a relief for MNEs remains to be seen.

The use of a European Cloud and thus a decoupling of EU-based data controllers from data processors in the US could lead to a promotion of data flow restrictions. These restrictions might also be an interest of data controllers to avoid raising efforts with the draft and implementation of MNE-internal data protection policies. A position of “Deutsche Telekom” highlighted the same tendency by stating the aim to

achieve data sovereignty by establishing an appropriate reference architecture that enables control and use of data based on clear frameworks. These frameworks should include mandatory certification to ensure security standards, interoperability specifications with regard to the services to be offered, and further requirements that could be imposed in each case depending on the criticality of the shared data (e.g., restriction to cloud services where access by non-European states can be ruled out on the basis of foreign legislation).¹⁶⁰⁵

An IAPP-EY Privacy Governance report showed that 10% of 473 MNEs have chosen to localize data, to stop transfers or to halt related services as a result of *Schrems II*; and that 4 in 10 MNEs said they have data and technology controls in place to restrict data transfers based on jurisdiction.¹⁶⁰⁶ Due to the significantly increased requirements under Chapter V of the GDPR, MNEs based in the US may block users with European IP addresses, reduce the information offered or only make it available for an additional charge, instead of adapting their own data protection policies to European requirements. A free flow of data, which is in principle of interest for MNEs, could therefore be thwarted by these actions and reactions within the digital economy.

Data controllers have an interest in the largest possible market for the demand side. However, this must be viewed in a more differentiated way for the supply side. At the beginning of the development of the Internet, services to access the Internet were still considered “basic services” and were therefore more regulated than today. In less regulated territorial areas such as the US or the UK, there was usually a monopoly or oligopoly with a clear market leader (e.g., AT&T, British Telecom). Due to their *de facto* market power, these data controllers had no interest in a competitive market on the supply side. In contrast, those that did not have access to this market for factual or regular reasons had such interest. As mentioned above¹⁶⁰⁷ in the context of the European Data Strategy, we find ourselves (again) in a similar situation today that consists of US-based ISPs and CSPs, being data controllers, having achieved *de facto* market power. The companies competing with them therefore have an increased interest in a regulated market to gain easier access to this market and to weaken the legal or *de facto* position of the strong companies as well as to reduce their economic position. There is therefore a constant potential for conflict between these types of SPs, which has implications for the stakeholders in the regulatory processes.

¹⁶⁰⁴ EDPB. Recommendation 01/2020 (Version 2.0). Paras. 13, 90 ff.

¹⁶⁰⁵ Deutsche Telekom AG. (1 July 2020). *Position der Deutschen Telekom zur EU-Ratspräsidentschaft Deutschlands*. <https://www.telekom.com/resource/blob/608208/2524892254e198e89bf07a5cdf9c61be/dl-position-telekom-zur-eu-ratspraesidentschaft-deutschlands-data.pdf>. P. 8.

¹⁶⁰⁶ LaLonde, B. [Brandon] and Thompson, M. [Mark] and Kanthasamy, S. [Saz]. (2021). *IAPP-EY Annual Privacy Governance Report 2021*. <https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2021>. P. 24–25.

¹⁶⁰⁷ See Chapter II, Section II.3.8.2.

A data controller can be determined as such in different jurisdictions at the same time under the applicable national regulations, because it might offer services directed to customers in a variety of jurisdictions. It might be subject to several legal frameworks at the same time for what is effectively one and the same TFPD scenario under one business model. Although data controllers might be concerned with the legally compliant design of their business models, the result of the efforts to reach compliance could go so far that it is practically impossible for a MNE to fully comply with all legal requirements applicable to the respective TFPD scenario.¹⁶⁰⁸ The determination of jurisdiction and applicable law to one legal entity alone often means a considerable effort in time and money, which can prove particularly problematic for SMEs. An IAPP-EY Privacy Governance Report showed that only 32% of 473 MNEs are able to categorize data subjects by jurisdiction and handle each data subject's data according to the law applicable.¹⁶⁰⁹ Substantive law in these jurisdictions can then differ considerably. This may then tempt data controllers to reduce or even ignore the rights of data subjects and the level of the European data protection framework.¹⁶¹⁰

Since the GDPR came into force, the attention about the protection of personal data has increased in SAs but also in the public opinion. In the event of non-compliance with the law, this could lead to "direct" and "indirect" financial implications, which data controllers want to avoid.

Direct implications can be fines that have been increased under the GDPR both in amount and frequency. In 2019, a case was raised by the French SA "Commission Nationale de l'Informatique et des Libertés" (CNIL) against Google.¹⁶¹¹ The fine, issued on 21 January 2019, stemmed from complaints filed by the Austrian organization NOYB and the French NGO "La Quadrature du Net". The subject of the complaints was the (obligatory) creation of a Google account during the configuration of a cell phone with the Android operating system. Google had been accused of not having a valid legal basis for processing personal data of users of its services, in particular that the lawfulness requirements were not met for profiling activities. The CNIL essentially followed this opinion and imposed a fine of EUR 50 million on Google for lack of transparency, information and legal basis in connection with data processing in the Android operating system. The Luxembourg SA imposed a fine of EUR 746 million on Amazon, both for violations of the GDPR.¹⁶¹² WhatsApp was also affected by direct financial implications. With notice dated 2 September 2021, the Irish SA announced a decision in the proceedings against WhatsApp, which had been initiated in December 2018.¹⁶¹³ Due to various violations of the GDPR, Facebook was to pay a fine of EUR 225 million. The CNIL fined Google EUR 150 million and Facebook EUR 60 million for violating rules of the E-Privacy Directive.¹⁶¹⁴ The Irish SA began investigating Meta's Irish subsidiary as a

¹⁶⁰⁸ Moerel, L. [Lokke]. (2012). *Binding Corporate Rules*. Oxford University Press. P. 88.

¹⁶⁰⁹ LaLonde, B. [Brandon] and Thompson, M. [Mark] and Kanthasamy, S. [Saz]. (2021). *IAPP-EY Annual Privacy Governance Report 2021*. <https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2021>. P. 22.

¹⁶¹⁰ Moerel, L. [Lokke]. (2012). *Binding Corporate Rules*. Oxford University Press. P. 22.

¹⁶¹¹ CNIL. (21 January 2019). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>. // EDPB. (21 January 2019). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

¹⁶¹² Manancourt, V. [Vincent]. (5 September 2022). *Instagram fined EUR 405M for violating kids' privacy*. *Politico*. <https://www.politico.eu/article/instagram-fined-e405m-for-violating-kids-privacy>. // Bodoni, S. [Stephanie]. (30 July 2021). *Amazon Gets Record USD 888 Million EU Fine Over Data Violations*. *Bloomberg*.

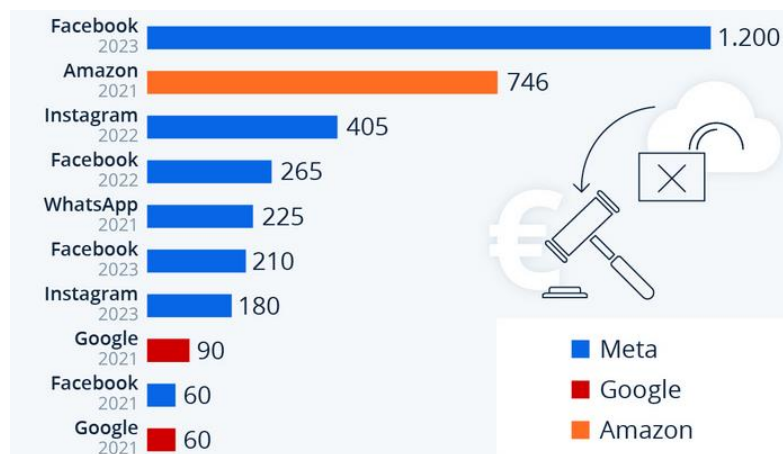
<https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach>.

¹⁶¹³ Irish Data Protection Commission. (2 September 2021). *Data Protection Commission announces decision in WhatsApp inquiry*. <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>.

¹⁶¹⁴ CNIL. (6 January 2022). *Cookies: la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros et FACEBOOK à hauteur de 60 millions d'euros pour non-respect de la loi*. <https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions>.

result of numerous data protection incidents reported by the company in 2018. The regulator found that Meta was unable to demonstrate the security measures it had taken to protect EU users' data in relation to 12 data protection incidents and fined the company with EUR 17 million based on an infringement of Arts. 5(2), 24(1) GDPR.¹⁶¹⁵ In late May 2023, after a binding dispute resolution decision by the EDPB, the Irish SA fined Meta with the highest fine to date for a breach of the GDPR at EUR 1.2 billion and ordered to suspend the transfer of data to the US, though Meta was given some months to implement the decision.¹⁶¹⁶ Microsoft is also affected by a draft decision by the Irish SA, with a proposed fine of approximately USD 425 million.¹⁶¹⁷

The highest fines are currently (as of 23 May 2023) distributed as follows:



Source: Statista, "Meta dominiert die DSGVO-Top 10"¹⁶¹⁸

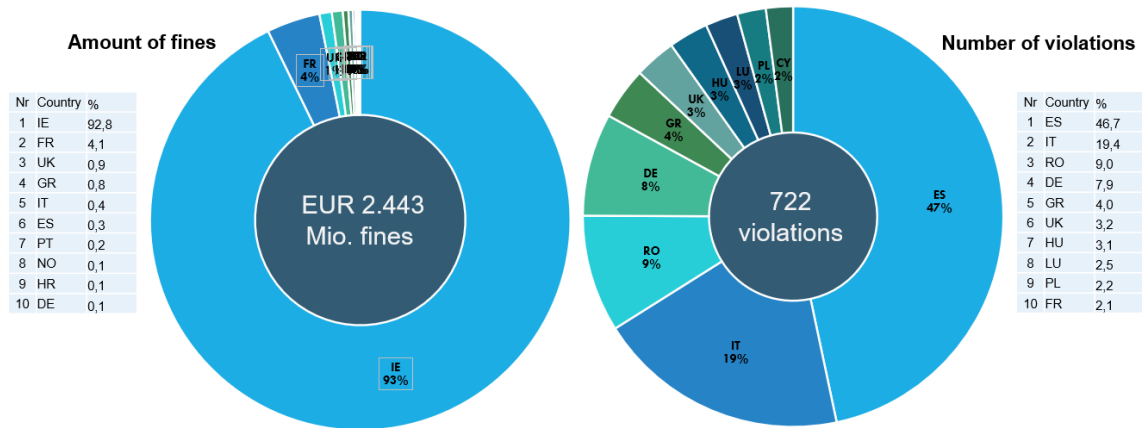
This influences the distribution of fines within the EU. In this context, the focus is primarily on the Irish SA, since most US tech companies have taken their European headquarters to Ireland. This highlights the following graphic:

¹⁶¹⁵ Irish Data Protection Commission. (15 March 2022). *Data Protection Commission announces decision in Meta (Facebook) inquiry*. <https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry>.

¹⁶¹⁶ EDPB, *1.2 billion euro fine for Facebook as a result of EDPB binding decision*, https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en. // Satariano, A. [Adam]. (22 May 2023). *Meta Fined \$1.3 Billion for Violating E.U. Data Privacy Rules*. *The New York Times*. <https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>. // *Nota bene*: This fine concerned GDPR rules. There was already a higher fine of EUR 1.49 billion against Google, however for breaching EU antitrust rules. // See also Chapter VIII., Section I.2.1.

¹⁶¹⁷ Gain, V. [Vish]. (1 June 2023). *Microsoft says Irish DPC intends to slam LinkedIn with a \$425m fine*. <https://www.siliconrepublic.com/business/microsoft-linkedin-fine-irish-data-protection-commission-gdpr-draft>.

¹⁶¹⁸ Statista GmbH. (2023). *Meta dominiert die DSGVO-Top 10*. <https://de.statista.com/infografik/25449/fuer-verstoesse-gegen-datenschutzgesetze-verhaengte-geldbussen/>.



Source of data (as of 1 June 2023): www.dsgvo-portal.de

The Commission is attempted¹⁶¹⁹ to address this imbalance with a new regulatory initiative which has been presented on 4 July 2023¹⁶²⁰. The plan is to restructure or reorganize the enforcement of data protection measures against companies operating across borders. The primary goal is a harmonized treatment of potential cases of violations of the GDPR.

Direct implications can also be that SAs, based on their rights and obligations described in more detail below¹⁶²¹, decide on a temporary or permanent restriction of transborder data transfers of a data controller. On 7 July 2022, the Irish SA changed a previously rather “data controller-friendly approach” to possible infringement actions and published a draft order to halt Meta’s transfers of personal data to the US. With this, the SA wants to prohibit Meta from continuing to store user data on its servers in the US. If was to get its way, this would probably mean, at least temporarily, that Instagram and Facebook could no longer be used from Europe. Meta repeatedly warned that such a decision would shutter many of its services in Europe, including Facebook and Instagram.¹⁶²² The Irish SA sent the draft decision to its counterparts in the other EU States, which could still influence the decision according to the Art. 60 GDPR procedure. There were various reactions to this, depending on the interests at stake; Norway, e.g., wanted Facebook fined for illegal data transfers.¹⁶²³ Maximilian Schrems, who filed the original complaint to the Irish SA, said at the time, “we expect other DPAs to issue objections, as some major issues are not dealt with in the DPC’s draft. This will lead to another draft and then a vote.”¹⁶²⁴

¹⁶¹⁹ European Commission. (24 February 2023). *Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en.

¹⁶²⁰ European Commission. *Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM(2023) 348 final*, (4 July 2023).

¹⁶²¹ Chapter IX, Section I.1.4.

¹⁶²² Manancourt, V. [Vincent]. (7 July 2022). Europe faces Facebook blackout. *Politico*. [https://www.politico.eu.cdn.ampproject.org/c/s/www.politico.eu/article/europe-faces-facebook-blackout-instagram-meta-data-protection/amp.//Bodoni, S. \[Stephanie\]. \(29 July 2022\). Meta Repeats Why It May Be Forced to Pull Facebook From EU \(1\). Bloomberg. https://news.bloomberglaw.com/privacy-and-data-security/meta-repeats-threat-it-may-pull-facebook-instagram-from-europe](https://www.politico.eu.cdn.ampproject.org/c/s/www.politico.eu/article/europe-faces-facebook-blackout-instagram-meta-data-protection/amp.//Bodoni, S. [Stephanie]. (29 July 2022). Meta Repeats Why It May Be Forced to Pull Facebook From EU (1). Bloomberg. https://news.bloomberglaw.com/privacy-and-data-security/meta-repeats-threat-it-may-pull-facebook-instagram-from-europe).

¹⁶²³ “There would be little or no incentive to act in accordance” with EU data transfer laws if regulators don’t impose a fine on the U.S. tech giant, Norway’s SA said”. See Manancourt, V. [Vincent]. (22 August 2022). Norway wants Facebook fined for illegal data transfers. *Politico*. <https://www.politico.eu/article/norway-wants-facebook-to-be-fined-for-illegal-data-transfers>.

¹⁶²⁴ Bracy, J. [Jedidiah]. (7 July 2022). *Irish DPC files draft order to halt Meta’s data transfers to US*. <https://iapp.org/news/a/irish-dpc-files-draft-order-to-halt-metas-data-transfers-to-us>.

Indirect implications are for example a loss of reputation and the value of stock exchange shares, which alone can be enough to do more damage to a data controller's reputation than a direct fine.

MNEs push for data protection requirements to be harmonized at both State and global level to reduce efforts to facilitate for their activities to be compliant with the applicable law. Early on in 2007, Google called for the creation of "Global Privacy Standards".¹⁶²⁵ Facebook also made its own suggestions, and its CEO Mark Zuckerberg spoke out in favor of such harmonization:

I believe that a common global framework – instead of regulation that differs greatly from country to country and from state to state – wants to ensure that the Internet is not broken and everyone receives the same protection.¹⁶²⁶

He also highlighted the EU data protection regulation as a role model for the world. With the EU claiming extraterritorial reach of the GDPR, US companies have constantly expressed concerns that clear and consistent guidelines for implementation and enforcement of the rules of the GDPR are required. In early 2022, Google was – through a ruling of the Austrian SA followed by other SAs¹⁶²⁷ – faced with the risk that the Google Analytics tool is not compatible with the supplementary measures of Art. 46(2)(c) GDR, which in the worst case could lead to a blocking of this tool by SAs in the Union. This led to Google's President of Global Affairs and Chief Legal Officer Kent Walker urging EU and US governments to finalize a successor to the Privacy Shield.¹⁶²⁸ Apple CEO Tim Cook emphasized in April 2022 again his company's mantra that privacy is a fundamental human right and added that "privacy is one of the most essential battles of our time".¹⁶²⁹ The focus of exemplarily those three MNEs nevertheless no longer lies only on preventing regulations, but also on influencing regulatory approaches to avoid "business-damaging" regulation as far as possible. This is also demonstrated by recent developments at US level, particularly well-illustrated in the wake of Connecticut's¹⁶³⁰ and North Dakota's¹⁶³¹ privacy legislation initiatives, where bills failed in the State house presumably through the influence of data controllers in these States.

Public authorities as controllers pursue the interest of fulfilling the purpose of the respective State. These purposes can be of various kinds and therefore cannot be considered here in their entirety. States pursue legitimate interests, especially those of national security, which they then pass on to their public authorities.

Every country in the world naturally has an interest in national security, but there are differences in the balancing of this interest. This is illustrated, for example, by the SWIFT agreement¹⁶³², which included that this national security interest has to be balanced

¹⁶²⁵ Google Public Policy Blog. (14 September 2007). *Call for global privacy standards*. <https://publicpolicy.googleblog.com/2007/09/call-for-global-privacy-standards.html>.

¹⁶²⁶ Zuckerberg, M. [Mark]. (30 March 2019). Opinion: Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas. *The Washington Post*. https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

¹⁶²⁷ See Chapter II, Section II.3.4.4.g.

¹⁶²⁸ Bryant, J. [Jennifer]. (20 January 2022). *Austrian DPA's Google Analytics decision could have "far-reaching implications"*. <https://iapp.org/news/a/far-reaching-implications-anticipated-with-austrian-dpas-google-analytics-decision>.

¹⁶²⁹ Bracy, J. [Jedidiah]. (12 April 2022). *Apple's Tim Cook: Protecting privacy most essential battle of our time*. <https://iapp.org/news/a/apples-tim-cook-protecting-privacy-most-essential-battle-of-our-time>.

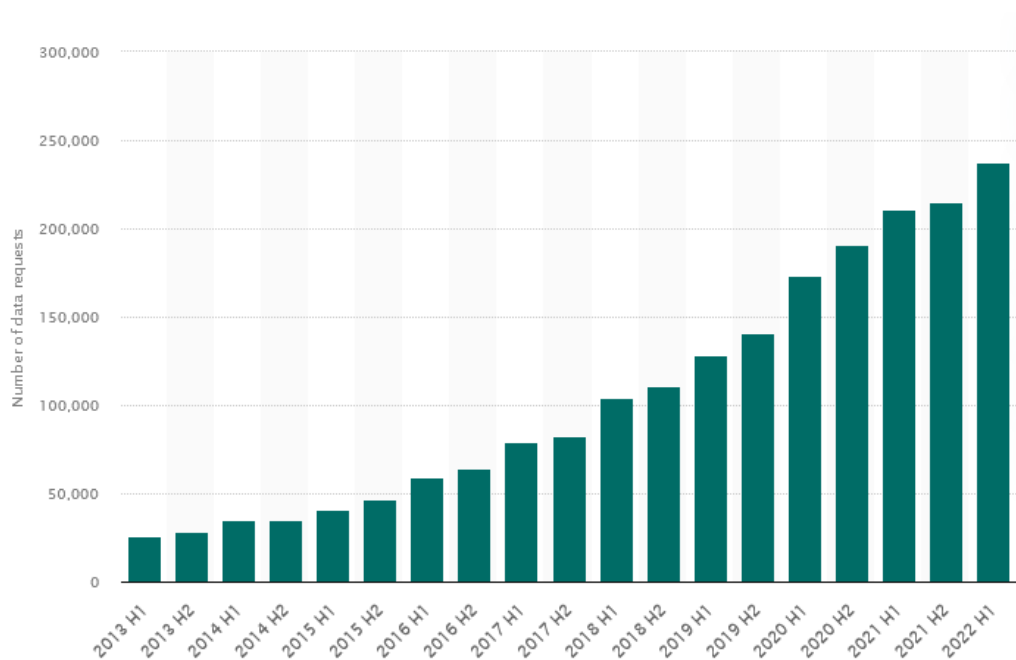
¹⁶³⁰ Feathers, T. [Todd]. (15 April 2021). *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*. <https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious>.

¹⁶³¹ Klosowski, T. [Thorin]. (6 September 2021). *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*. *The New York Times*. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us>.

¹⁶³² See also Chapter II, Section II.4.1.

against the data protection interest of the individual.¹⁶³³ The ongoing criticism of the SWIFT agreement shows how the right to data protection as an interest has gained in importance in the meantime, even compared to the security interest. In *Schrems I*, the CJEU already criticized the predominance of US security interests over European data protection interests.¹⁶³⁴ The CJEU found access possibilities of public authorities to the personal data transferred to be too far-reaching. Authorities as data controllers may therefore have legitimate national security interests, but these must be weighed against the interests of the individuals.

Closely linked to this interest are investigatory and enforcement interests. These have increased compared to SPs, especially VLOPS, in recent years, as the following chart exemplifies using Facebook.



Source: Statista, “Number of user data requests issued to Facebook by federal agencies and governments worldwide as of 1st half 2022”¹⁶³⁵

A distinction between these interests, as well as between investigations regarding “criminal” and “non-criminal” actions, remains difficult, which has shown the analysis of the scopes of the LED¹⁶³⁶ and the E-Evidence package¹⁶³⁷. For scoping purposes, both purposes shall be subordinated to the interest of public order. In this area, too, a variety of interests of a data controller must be brought into practical concordance with others: Law enforcement interests, data protection interests of defendants and particularly vulnerable persons, sovereignty interests of the States in which the personal data in question are located, and interests of the providers. Authorities may request personal data from third Parties in pursuit of these interests. These third Parties may be legal entities or other public authorities.

¹⁶³³ EU. *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program*, OJ L 195, 5-14, (27 July 2010). Recital 7

¹⁶³⁴ *Schrems I*, Para. 84 ff.

¹⁶³⁵ Statista GmbH. (8 February 2023). *Number of user data requests issued to Facebook by federal agencies and governments worldwide as of 1st half 2022*. <https://www.statista.com/statistics/277230/facebooks-global-user-data-requests/>

¹⁶³⁶ See Chapter I, Section I.2.3.5.

¹⁶³⁷ See Chapter I, Section I.2.3.7.

Providers, if requested to produce personal data for the interest of public order, might then find themselves in a conflict of compliance with two laws. On the one hand, the law where the requesting authority is located; on the other hand, all the national laws applicable to the data subjects whose personal data this provider processes. The legal review of those laws by the affected providers might be complicated by the fact that the order may involve criminal offenses that are regulated differently in the national legal systems to be reviewed, especially if a short period of time is set for the fulfillment of such order. Therefore, providers have an interest in uniformly regulated “checks & balances” to prevent disproportionate data access and thus an interference with potentially many relevant national laws, and therein in particular fundamental rights protections. This uniformity is difficult to achieve in the example of the E-Evidence Regulation, even in a territorially limited supranational order such as the European framework, as rules in the Member States regarding, e.g., the deletion periods for telecommunications data continue to be inconsistent. Providers can therefore be faced with the expense of reviewing legal systems different from their place of incorporation and the location of their principal place of business. Data controllers may also be confronted with ambiguities about foreign authorities being entitled to issue orders to produce personal data. Usually, the judicial authorities of the country in which the provider is domiciled are not informed and involved, which is contradictory to this procedural corrective. Whether or not the legality of such order is reviewed usually depends on the legal reaction (e.g., objection against the order) of the provider. Future regulations would therefore have to be formulated in such a way that they guarantee data controllers a high degree of legal certainty. Otherwise, they would be exposed to a double risk: if a data controller does not produce the requested data, he may face sanctions for obstruction of justice. However, if the controller produces the requested data, data subjects may claim damages if it turned out that the conditions for the production had not been met after all. Clear rules are therefore needed, both regarding the national authorities’ powers to order the production of data and the types of criminal offenses in which transborder orders can be issued.

For public authorities, immediate access to personal data stored in another country (or in the case of cloud scenarios, in many countries) is important to access procedurally relevant data in a digitalized world and to guarantee the effective and fair administration of criminal justice. However, such access to these data has so far only been possible in exceptional cases (e.g., publicly accessible data or with the consent under Art. 32 of the Cybercrime Convention). In principle, a request for mutual legal assistance to the foreign State is then necessary. However, this procedure is, on the one hand, lengthy and, on the other hand, dependent on the existence of corresponding MLATs and the will as well as the possibilities of the local law enforcement authorities, which simply could not provide necessary resources. The possibilities of the existing legal instruments (e.g., MLATs) are therefore presumably not exhausted from the point of view of the authorities concerned.

Access opportunities are often unevenly distributed within digital value creation systems. Resulting so-called “data oligopolies” are increasingly perceived as an obstacle to innovation, competition and public welfare. Various stakeholders, including the European Commission, have come forward with plans to remedy this situation. The Commission wants to – outlined in its Data Strategy¹⁶³⁸ – focus on the use of large amounts of data to improve innovation and competition. The Commission focuses on the promotion of “open data”. Open data regulations pursue a bundle of interests: the creation of transparency and thus the control and safeguarding of government action relevant to the common good, better citizen participation, the emergence of new markets, and ultimately

¹⁶³⁸ See Chapter II, Section II.3.8.2.

the promotion of innovation and competition. The Open Data Directive extends the scope of the rules on the re-use of public sector information beyond the public sector and now also includes public companies. In principle, all documents made accessible by public sector bodies should be able to be reused for any purpose, provided they are not protected by third-party rights. This means that personal data can consequently only be published if there is a legal basis for this processing step.

1.2. Data (sub-)processors

Schrems II manifested the obligation for those responsible for a TFPD to assess the level of data protection in the third country by a TIA¹⁶³⁹. Processors are therefore on an equal footing with data controllers in this obligation. In addition, they are dependent on their respective data controller due to the contractual relationship and have an obligation to assist in ensuring the protection of the rights of data subjects. On the other hand, in the case of onward transfers, they are obliged to extend the obligations arising from the controller-processor relationship to their sub-processors. This can result in a considerable administrative effort and an increased exposure to financial implications, both in the internal relationship with the data sub-processor and data controller, as well as in the relationship with SAs, with other public authorities, and with data subjects. Apart from that, the same as mentioned above¹⁶⁴⁰ regarding data controllers interests applies to (sub)processors.

1.3. Data subjects

Data subjects are interested in a transborder use of digital services. The digital world offering these services thrives on private impulses for technical and economic innovations. Ultimately, these also benefit the data subjects. One example is the model of free services offered by Facebook, Google, YouTube, WhatsApp, Skype, etc., which are primarily financed by advertising revenues. Data subjects are therefore end users of the transborder data flow and regularly depend on appearing on the market as service users. Service users are therefore consumers with explicit consumer interests in a sufficient supply of services, interests in transparency of their market, interests in the quality of the services offered and in favorable conditions and costs of service on that market. This also implies interests in a certain degree of competition among providers on the market. To fulfill these interests, they often prefer services free of charge, and in many cases do not attach great importance to data protection law, as especially representatives of the “post privacy” movement¹⁶⁴¹ use to point out. However, the TFPD can not only affect the interests of service users but also the interests of third Parties who are not involved in these services and whose personal data become objects of a use of such service.

Like data controllers and data (sub)processors, data subjects are also interested in a free flow of data. This free flow can be impeded in various ways that collide with the interests of the data subjects. For data subjects, regulatory interventions can also be of importance, but their criticism, at least at the beginning of the Internet Era, was essentially directed against restrictions on access to services. Nowadays, as the OECD pointed out, this has been shifted towards a

¹⁶³⁹ See also Chapter II, Section II.3.4.4.g.

¹⁶⁴⁰ Chapter IX, Section I.1.1.

¹⁶⁴¹ See also Chapter VI, Section I.

strong business case for privacy protection. [...] With the growing collection of personal data, the risks to individual privacy increase, which is why consumers are increasingly asking for assurances that their data are being handled appropriately. Businesses increasingly see their ability to meet these demands as part of their competitive offering.¹⁶⁴²

Public knowledge that data protection has a fundamental rights aspect and includes certain remedies to act against violations of their rights in this area of law has enhanced. Iakovleva summarized that

although individuals can gain from the free flow and ubiquitous monetization of their data by companies – for example, in the form of personalized services – they also have a lot to lose. From a global perspective, massive cross-border appropriation of personal data has been compared to resource extraction. Potential damage to individuals, and to society as a whole, far transcends the direct economic losses suffered from data breaches and identity threats.¹⁶⁴³

Similarly, the OECD found a loss of control to be one of the main concerns of consumers:

With a growing online presence, more opportunities to record our activities arise, leading to a higher probability of revealing facets of ourselves that we may wish not to share with a company hence fueling concerns about privacy protection. Moreover, additional concerns arise when the data gathered is monetized in another form, such as by selling it to other firms who may make use of it for marketing or other purposes.¹⁶⁴⁴

Data subjects have therefore an increasing interest in ensuring that their fundamental rights are not sacrificed to interests of private companies as well as public authorities. The German Constitutional Court formulated the urgency of this concern in its “*Volkszählungsurteil*” judgment, whose findings apply just as much to the Internet, where much of today’s communication takes place – and thus much of the data subjects’ daily lives:

Anyone who is unsure whether deviant behavior will be noted at any time and permanently stored, used or passed on as information will try to avoid attracting attention through such behavior. Anyone who expects that participation in a meeting or a citizens’ initiative, for example, will be recorded by the authorities and that this may cause them risks will possibly refrain from exercising their corresponding fundamental rights (Arts. 8 and 9 of the *Grundgesetz*). This would not only impair the individual’s opportunities for development, but also the common good, because self-determination is an elementary functional condition of a free democratic community based on the ability of its citizens to act and participate.¹⁶⁴⁵

During these “actions” and “participations”, data subjects are concerned that their rights might be disproportionately impaired, even when using free services. Data subjects assign to stakeholders in regulatory processes a duty to define proportionality and to ensure that this is complied with by means of positive and negative obligations¹⁶⁴⁶ of the State to protect its citizens. Data subjects are also increasingly aware that a global

¹⁶⁴² OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 32.

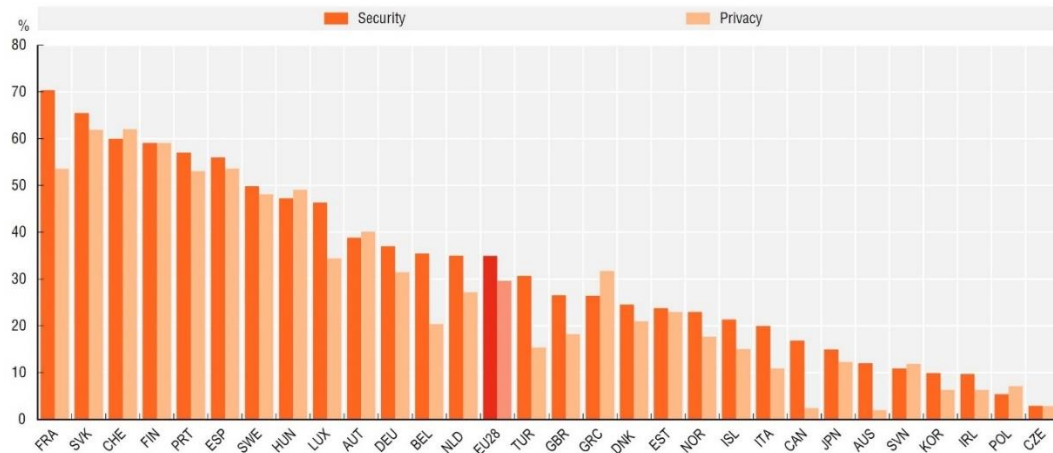
¹⁶⁴³ Iakovleva, S. [Svetlana]. (2021). *Governing cross-border data flows: Reconciling EU data protection and international trade law*. [Doctoral thesis, Faculty of Law, Universiteit van Amsterdam (I. Venzke)]. <https://hdl.handle.net/11245.1/cf54d2a9-cd41-42c2-94f1-24c81f8a3abd>. P. 311.

¹⁶⁴⁴ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 31.

¹⁶⁴⁵ German Federal Constitutional Court. *Judgment of the First Senate of 15 December 1983*, 1 BvR 209/83, 1–215. Para. 146.

¹⁶⁴⁶ See below Chapter IX, Section I.2.1.

ecosystem of transborder data flows is complex. Nevertheless, the general public tends to understand that there has to be some kind of “balance” between the advantages of the digital transformation and fundamental rights, that this balance is not easy to find and can vary according to individual preferences.¹⁶⁴⁷ These preferences can differ significantly depending on a culture population’s basic attitude, as the following graphic shows.



Source: OECD, “Main reasons for not buying online because of privacy and security concerns”¹⁶⁴⁸

The balancing from a regulatory perspective is therefore dependent on many factors, and robust criteria for proportionality aspects inside regulatory measures on a global level are difficult to achieve. Perry & Roda stated in this respect that

as we reflect on how we are going to live with new technology in the decades to come, balance is the key component in our evaluation of the costs and benefits of the digital revolution. The digital tightrope – a balancing act between breakneck technological development on the one side, countered by unforeseen consequences that may promote or violate time-honored rights on the other – represents a conundrum for humans, both as individuals and as collective.¹⁶⁴⁹

This balance becomes the more important the more sensitive personal data are. The GDPR has included this in Art. 9. The processing of sensitive personal data on the basis of a public interest must be proportionate in each individual case. Thus, the data processing must aim at a substantial public interest, it must be suitable and necessary to achieve it, and the disadvantages caused must be proportionate to the aim. Overall, a strict standard must be applied, especially due to the importance of sensitive data for the fundamental rights of Arts. 7, 8 of the Charter.

National laws provide for legal consequences if a breach of a national data protection provision is established. Such breach can lead to a claim for damages by the data subject in accordance with the general provisions of contract law, tort law, and special liability statutes. However, individual legal enforcement still has little practical significance. The data processing procedures of a company operating on the Internet, for example, can hardly be viewed and understood by data subjects being “outsiders” of the details of those TFPD scenarios. In addition, the effort of judicial redress is seldom outweighed by

¹⁶⁴⁷ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 31.

¹⁶⁴⁸ OECD. (16 September 2014). *OECD computations based on Eurostat, Information Society Statistics and national sources*. <http://dx.doi.org/10.1787/888933148160>.

¹⁶⁴⁹ Perry, S. [Susan] and Roda, C. [Claudia]. (2017). *Human Rights and Digital Technology*. Palgrave Macmillan. P. 191.

the potential amount of damages. In practice, moreover, there is no guarantee that personal data from data subjects will not be transferred to parts of the world where there is no adequate level of protection. Effective data protection can only be ensured if data subjects also experience sufficient protection outside their own national borders.

1.4. Supervisory Authorities and Data Protection Officers

SAs and DPOs have a position as intermediaries in the global ecosystem of transborder data flows. They have both factual influences on TFPD scenarios as well as on regulatory processes. The main interest of SAs lies in the compliance with their duties and the enforcement of their powers. To fulfill their duties, the SAs have certain powers vis-à-vis data controllers, set out, e.g., by Arts. 58(1) and 58(2) GDPR.

SAs must advise the national parliament, government, as well as other institutions and bodies on legislative and administrative measures to protect the rights and freedoms of natural persons in relation to the processing of personal data and cooperate and provide assistance to other SAs to ensure the consistent application and enforcement of regulations such as the GDPR; this manifests the influence of SAs on regulatory processes. Another power lies in the enforcement of fines. As the example of the UK shows, SAs are increasingly interested in (re)financing themselves through such fines.¹⁶⁵⁰

Another power lies in the temporary or permanent restriction of TFPD, including a prohibition of future transfers. As Naef correctly noted, the CJEU

explicitly stated that the exercise of the powers to suspend and prohibit data transfers set out in Article 58(2)(f) and (j) GDPR are not simply optional, but an obligation that the supervisory authorities in the EU member states have to fulfill in cases in which the level of protection required by EU law cannot be ensured. [...] In the end, it is the individual supervisory authorities of the EU member states that are responsible for enforcing the right to continuous protection of personal data in Article 8 CFR.¹⁶⁵¹

After *Schrems I* and *Schrems II*, each time there was a phase of legal uncertainty also for SAs regarding the further handling of the legal situation. After *Schrems II*, SAs have commented on the judgment of the CJEU and have each determined, for their jurisdiction, which requirements from the perspective of the SAs must be observed in the event of a TFPD to third countries. There were differing opinions as to whether data transfers to third countries outside the EU/EEA would be possible based on appropriate safeguards. This led to a fragmentation into high, average, or low requirements to implement the findings of *Schrems II*.¹⁶⁵² This contradicted that “supervisory authorities must act to remedy violations of the right to continuous protection of personal data, and they must act consistently”¹⁶⁵³.

The EDPB also recognized this danger and adopted a document to provide stakeholders with guidance on the use of legal instruments for the transfer of personal data to third

¹⁶⁵⁰ United Kingdom, Information Commissioners’ Office. (14 June 2022). *ICO funding update: Fine income retention agreement*. <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/ico-funding-update-fine-income-retention-agreement>.

¹⁶⁵¹ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 426.

¹⁶⁵² Matthiesen, R. [Reemt] and Heinzke, P. [Philippe] and Dreyer, J. [Julia]. (9 April 2021). *Schrems II: Reaktionen auf das Urteil und Empfehlungen der Aufsichtsbehörden – Update #23*. *CMS Deutschland*. <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/schrems-ii-aufsichtsbehoerde-standardvertragsklausel-scc>.

¹⁶⁵³ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 426.

countries, including the US.¹⁶⁵⁴ As a result of the lack of transparency in the digital space, it is often challenging for the SAs to detect violations of the law, even in the case of a data controller based in Germany. In the absence of proof, they cannot be sanctioned, which means that in practice, especially in transborder cases, the possibilities for sanctions are rarely realized. Transparency of data processing and sufficient enforcement powers are thus further interests of SAs.

SAs also have an interest in keeping the bureaucratic burden of their activities to a minimum. With the entry into force of the GDPR, this burden was reduced insofar as data transfers based on SDPC or BCR no longer must be notified in advance to the SAs and to be approved by them. The GDPR retained nevertheless the option for companies to use approved CoCs or certification procedures to provide appropriate safeguards under certain conditions.

Due to the “one-stop-shop” mechanism¹⁶⁵⁵ stipulated in Art. 56 GDPR, a lead SA can become the sole contact for those responsible for the processing, which means that only actions of the lead SA have binding effects. Since several MNEs, e.g., Google, and Facebook, have their European offices in Dublin, the Irish SA had been inundated with requests and complaints since the GDPR became effective. The EDPS estimates that “95% of data protection cases in Europe are at the local level” and “less numerous, cross-border cases can have far-reaching consequences for millions of data subjects and affect tens of other cases”.¹⁶⁵⁶ This is not yet a problem, as this is precisely what the GDPR provides for. However, the Irish SA seems to have substantial problems with the processing of such cases. According to the Irish Council for Civil Liberties (ICCL), the Irish data protection SA has completed just 2% of all procedures since May 2018.¹⁶⁵⁷ SAs are therefore interested to avoid such an overload.

Nevertheless, cooperative governance is not the only concern but also the national administrative procedures. The IAPP argued that “in national legislation, there are sometimes differences so significant as to touch upon even what is a final complaint decision. National procedural law is very precise, whereas the DPAs could only refer to some vague principles of the GDPR as the data protection law does not address these procedural issues.”¹⁶⁵⁸ The EDPS and the German federal Commissioner for data protection and freedom of information therefore encouraged that it would be up to the European Commission to intervene to streamline administrative procedures.¹⁶⁵⁹ Others argued that “discrepancies in procedural law can be solved by the DPAs simply by ignoring national procedures that hamper the effective application of the GDPR, since European law takes priority over national rules”¹⁶⁶⁰.

Cooperation between the European SAs is based on Art. 60 GDPR. If no consensus is reached in this procedure, a so-called “coherence procedure” is initiated, Arts. 63 and Art. 65 GDPR. The French CNIL had already made several decisions against Google.

¹⁶⁵⁴ EDPB. (23 July 2020). *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*. https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

¹⁶⁵⁵ See also Chapter II, Section II.3.4.2.

¹⁶⁵⁶ Bertuzzi, L. [Luca]. (28 June 2022). *10 years after: The EU's 'crunch time' on GDPR enforcement*. <https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement>.

¹⁶⁵⁷ Irish Council for Civil Liberties. (9 April 2021). *Economic & Reputational Risk of the DPC's Failure to Uphold EU Data Rights*. <https://www.iccl.ie/digital-data/economic-reputational-risk-of-the-dpcs-failure-to-uphold-eu-data-rights>.

¹⁶⁵⁸ Bertuzzi, L. [Luca]. (28 June 2022). *10 years after: The EU's 'crunch time' on GDPR enforcement*. <https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement>.

¹⁶⁵⁹ Bertuzzi, L. [Luca]. (28 June 2022). *10 years after: The EU's 'crunch time' on GDPR enforcement*. <https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement>.

¹⁶⁶⁰ Bertuzzi, L. [Luca]. (28 June 2022). *10 years after: The EU's 'crunch time' on GDPR enforcement*. <https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement>.

The CNIL affirmed having jurisdiction to sanction violations of the GDPR by Google and thus rejected the use of the one-stop-shop mechanism. Google Ireland Ltd. is Google's European headquarters, but in terms of data protection law, it is not the main branch within the meaning of Art. 4(16) GDPR, since, in the opinion of the CNIL, essential decisions regarding the purposes and means of data processing are not made in Ireland. This threatened the one-stop-shop mechanism, led to discussions within the European framework and finally resulted in a guideline by the EDPB.¹⁶⁶¹ This guideline deals with the interactions between SAs under Art. 60 GDPR. The aim is to analyze the cooperation procedure and provide guidance on the concrete application of the provisions. In principle, the cooperation procedure applies to all transborder cases. In this context, the lead SA of a nation is primarily responsible for the procedure. The cooperation procedure does nevertheless not affect the independence of the SAs. They retain their own discretionary powers within the framework of cooperation.

The GDPR allows for the development of international cooperation mechanisms to facilitate the enforcement of data protection rules, including through MLATs. This recognizes the interest of SAs in establishing closer cooperation among SAs to provide both more effective protection of individual rights and greater legal certainty for businesses. Within the European framework, an EDPB's decision set up a "Coordinated Enforcement Framework" (CEF) in October 2020, together with the creation of a "Support Pool of Experts" (SPE).¹⁶⁶² Both are key actions of the EDPB under its 2021-2023 Strategy¹⁶⁶³. In early 2022, a launch of coordinated enforcement of public sector use of the cloud was announced as first coordinated action within the CEF,¹⁶⁶⁴ and EDPB Members agreed to further enhance cooperation on strategic cases that fulfil specific quantitative and qualitative criteria and to diversify the range of cooperation methods used.¹⁶⁶⁵ In September 2022, the EDPB proposed an EU Police Cooperation Code, which aims to enhance law enforcement cooperation across Member States, in particular the information exchange between the competent authorities.¹⁶⁶⁶ Through these measures, the European SAs want to counter criticism that the system is "too laborious and taking too long to deliver on time-sensitive decisions. [...] There is always a learning curve, although the digital environment requires regulators to act much faster"¹⁶⁶⁷.

The DPO is factually involved in the data flow, if the processing, in particular the use of new technologies, is likely to present a high risk to the rights and freedoms of natural persons by virtue of the nature, scope, context and purposes of the processing, as he must assess the consequences thereof in advance of the processing (Art. 35 GDPR). However, the DPO also completes the regulatory ecosystem by having further obligations under Art. 39 GDPR and, if applicable, being personally liable for his misconduct:

- He must inform and advise the controller or processor as well as the employees who process personal data about their obligations with regard to data protection.

¹⁶⁶¹ EDPB. (14 March 2022). *Guidelines 02/2022 on the application of Article 60 GDPR*. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022022-application-article-60-gdpr_en.

¹⁶⁶² EDPB. (20 October 2020). *EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679*. https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en.

¹⁶⁶³ See Chapter IX, Section II.3.

¹⁶⁶⁴ EDPB. (15 February 2022). *Launch of coordinated enforcement on use of cloud by public sector*. https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en.

¹⁶⁶⁵ EDPB. (29 April 2022). *DPA's decide on closer cooperation for strategic files*. https://edpb.europa.eu/news/news/2022/dpas-decide-closer-cooperation-strategic-files_en.

¹⁶⁶⁶ EDPB. (14 September 2022). *EDPB adopts statement on European Police Cooperation Code & picks topic for next coordinated action*. https://edpb.europa.eu/news/news/2022/edpb-adopts-statement-european-police-cooperation-code-picks-topic-next-coordinated_en.

¹⁶⁶⁷ Bertuzzi, L. [Luca]. (28 June 2022). *10 years after: The EU's 'crunch time' on GDPR enforcement*. <https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement>.

- He shall monitor compliance with the requirements of the GDPR and other Union or Member State regulations on data protection, as well as data protection policies, including the allocation of responsibilities, awareness raising and training of employees, and reviews in this regard.
- In performing his or her duties, the DPO shall take due account of the risks associated with the processing operations. In doing so, he or she shall take into account the nature, circumstances and purposes of the processing.
- A jointly appointed DPO of a group of companies shall be easily accessible from each branch.

The DPO will therefore be concerned, on the one hand, to be able to perform these duties in an environment of legal certainty. The controller must involve the DPO at an early stage in all matters relating to the protection of personal data. The DPO is assigned to this controller and naturally represents the interests of this controller. The GDPR brought with it comprehensive obligations for those responsible for the processing. These must not only ensure that they comply with the requirements of the GDPR but must also be able to prove that they are implementing appropriate data protection policies and suitable data protection precautions. Those responsible therefore started introducing so-called “data protection programs”, in which the organizational distribution of data protection is regulated. In this organization, the DPO is usually assigned to the so-called “second line of defense” – a term which stems from the general principles of IT governance – and must monitor and advise the “first line of defense”.¹⁶⁶⁸ Within this first line of defense, the majority of the employees of the controller or processor is located, which have all their own interests as data subjects. This often brings the DPO into conflict between his/her interests and those of all data subjects within the legal entity he is assigned to.

The DPO shall also cooperate with the SAs. He/she shall act as a contact person for the SA in matters related to data processing. He/she shall also be available to the SA for advice on any other issues. The DPO is therefore involved in the enforcement of the law; with regard to his/her interests in this function, what was said above about SA applies.

2. Stakeholders of a regulatory process

Stakeholders have in this thesis so far been depicted according to their functions within TFPD scenarios. However, in the regulatory reality, these stakeholders do not appear in these typified roles. This reality is rather characterized by a wide variety of forums in which interests are articulated and seek to influence decision-making processes. From the perspective of the international order, the aim within this reality is to manage conflicts in such a way as to maintain the stability of that order while at the same time deterring future violations of rules. This is naturally in tension with purely national strategies aimed at maximizing national interests. The main forums in which the regulatory stakeholders organize themselves, cooperate with each other and try to agree on forms of regulating TFPD within the international order, belong to the State level on the one hand, and to the international level on the other, whereby for this thesis supranational entities such as the EU are to be located at the State level.

¹⁶⁶⁸ Further details on the three lines of defense in Ho, A. [Amelia]. (1 July 2018). *Roles of Three Lines of Defense for Information Security and Governance*. <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance>.

2.1. National and supranational level

In industrialized countries and in several emerging economies, both public and private sectors have increased the use of information technologies, with personal data more and more being processed abroad. As a result, the internal sovereignty of States, their ability to solve economic, political, social, and cultural problems of society and to guide the prospects of societal development through domestically available information and processing resources, is affected the more the dependence on transborder data flows extends.

The significance of this dependence oscillates between light and heavy according to the “group” a particular State belongs to. The first group is made up of the US alone. Its position as home-country of an extensive data-driven industry is unique, which creates its fundamental interest in the export of services and equipment. The essential interests of other States, in turn, include access to data which is processed in the US. The other western industrialized States build the second group. They have a significantly weaker position as producers of data and services as well as hardware. They depend to a significant extent on imports of data, services, and hardware from the US. The emerging economies comprise the third group. The States within this group are the most loosely allied, taking divergent positions in the field of transborder data flows. Brazil, for example, designed regulation to foster the development of the country’s own computer and information industry.¹⁶⁶⁹ Other countries of this group decided to develop into services trading centers by opening their borders. Most of the fourth group, the developing countries, face a technological gap. They have a strong interest in access to information and technology, partly, but not only for military reasons, a consideration which can prompt western countries to deny access to their resources. It has become a development policy question whether and to what extent States of this fourth group acquire the technology necessary to be included in transborder data flows. Data processing capabilities are generally in hands of the industrialized countries, the developing countries are therefore not the “masters of information” concerning their national resources. There is therefore a constant danger that States of this fourth group could become the object of transborder data flows rather than benefiting from it.

In its positive obligation to protect its citizens – besides the negative obligation, a State has an

obligation exercise due diligence to take such preventive measures as the enactment of legislation and the establishment of regulatory and monitoring mechanisms aimed at preventing occurrences of human rights violations. The State must also take reactive measures once the violations have taken place. As a result, the reach of human rights to non-State conduct has been extended more than under the traditional conception of State responsibility. Unlike the latter, where proof of State action was required, responsibility falls on the State for violations of human rights by non-State actors even though the acts violating the rights have no direct or indirect correlation to the State. The State’s responsibility springs from the State’s actions or inactions before and after the violations, not necessarily from the physical violations themselves. Therefore, where violations of human rights occur because of conduct which cannot be classified

¹⁶⁶⁹ OECD. (2020). *Going Digital in Brazil, Chapter 6. Fostering the digital transformation of the Brazilian economy*. <https://www.oecd-ilibrary.org/sites/4f5ebe9d-en/index.html?itemId=/content/component/4f5ebe9d-en>.

as State action, the State might still be held responsible for them if it can be established that it failed to prevent or redress those violations.¹⁶⁷⁰

This also applies to a State's actions or omissions against foreign stakeholders. At a time influenced by the Internet, in which the importance of the State for modern political life and governance, especially vis-à-vis non-State actors, is increasingly diminishing, it is becoming more and more important for the State to fulfill its duties at the national but also international level. A State can therefore no longer influence the digital environment under its jurisdiction independently from global developments but needs to adapt its national plans to these developments for meeting its obligations. This could foster a State's distrust in developments emanating from global power shifts. Such a distrust could also have been caused by the fact that the State as such found itself in an "opposing current of thought on the role of the State"¹⁶⁷¹ in the context of the development of the global digital economy. As Chirwa also correctly noted,

international human rights law has imposed a responsibility on States which operates in binary opposition to the liberal conception of the State which dominates current global economic thought, as reflected in the notion of globalization demanding a minimal, non-interventionist State. [...] States in the globalizing environment [...] are supposed to adopt a *laissez-faire* approach, allowing the rules of the market to reign in economics and international trade, with minimal regulation of the private sector.¹⁶⁷²

This was certainly true until 2010, but since then a power shift has taken place, influenced by world trade, as China became first time the world's biggest goods exporter in 2010. This led to a rethinking and stronger criticism of such a *laissez-faire* approach. The credit crunch and the global recession after 2009 did the rest. Nevertheless, due to aforementioned obligations of the State, the (diminished, but still existing) opposing current, and the considerable resources a State would need to involve establishing an effective legal framework under these circumstances, national regulatory stakeholders usually focus first on their national policy capabilities.

These are primarily assigned to the following areas of a State's regulatory interest: security policy, economic policy, infrastructure policy and legal policy. It should also be noted that even within the stakeholder "State" it is not sufficient to include only certain parts of a government, but rather to include the whole-of-government, because silo solutions might not lead to a sustainable solution, which UNCTAD also noted:

Regulations on cross-border data flows can be found in different kinds of laws and regulations. The various examples of domestic regulations on cross-border data flows discussed in this chapter include data protection laws; cybersecurity laws, regulations and policies; Internet laws and regulations; regulations pertaining to both hardware and software; government procurement laws; laws related to protecting State secrets; income tax laws; corporate and accounting laws and regulations; policies related to e-commerce and digital development; and data strategies. Thus, as different areas of policymaking are involved, regulating in a silo approach may lead to inconsistent

¹⁶⁷⁰ Chirwa, D. [Danwood]. (2019). State Responsibility for Human Rights. In M. [Manisuli] Ssenyonjo, *International Human Rights Law. Six Decades after the UDHR and Beyond* (pp. 397–410). Routledge. P. 406-407.

¹⁶⁷¹ Chirwa, D. [Danwood]. (2019). State Responsibility for Human Rights. In M. [Manisuli] Ssenyonjo, *International Human Rights Law. Six Decades after the UDHR and Beyond* (pp. 397–410). Routledge. P. 407.

¹⁶⁷² Chirwa, D. [Danwood]. (2019). State Responsibility for Human Rights. In M. [Manisuli] Ssenyonjo, *International Human Rights Law. Six Decades after the UDHR and Beyond* (pp. 397–410). Routledge. P. 407.

measures in different ministries. This would call for a whole-of-government approach in regard to the governance of cross-border data flows.¹⁶⁷³

For all States with strong political and economic interdependence, the phenomenon of increasing transborder data flows has led to new challenges in security policy. Dependence on transborder data flows can lead to an increased vulnerability of national interests. This has given rise to numerous measures by States.

States could declare themselves to face a state of defense or state of emergency and use those as justification for their acts. As a concept in State responsibility, the state of emergency is not beyond dispute as grounds for justification. Self-defense, preemptive to an attack, signifies a gray area for the regulatory side, because this situation often does not allow a clear and quick judgment of the actual justification. States that have been attacked, are about to be attacked, or have jurisdiction where attacks have been perpetrated, could have due diligence obligations imposed on them *vis-à-vis* third States.

The economic and military dominance of the US after the end of World War II shaped elements of the international order. Within this order, however, a pluralistic liberal model and the convergence of States in the transatlantic community of nations equally influenced national interests. The national security strategies of the US have therefore been linked – with some temporary deviations – to concerns of the international community and to solidarity-based elements such as the promotion of development (earliest example: the so-called “Marshall Plan”). Later, however, the US’ invocation of national security became an extended pattern of argumentation to justify measures, especially after the 9/11 attacks. The US IC used national security, especially the “war on terror”, to justify bulk collection of personal data. This practice has been increasingly criticized after the NSA affair and influenced US citizen’s opposition to surveillance.¹⁶⁷⁴ On 12 December 2013, a committee report by the NSA Review Group¹⁶⁷⁵ concluded that the NSA was overreaching and that American civil liberties were at risk, “eroding a bit the US Constitution”¹⁶⁷⁶. In September 2020, a US court ruled that this type of collection by the NSA was unlawful and possibly unconstitutional.¹⁶⁷⁷ The court called the “extremely large number of individuals” from whom the NSA collected data “problematic”. In the years after the NSA affair, the national security justification therefore lost weight, at least within US borders. This national security interest collides with the interests of the data subjects, as Snowden also stated:

They had stolen and were stealing, not just one person’s memories, they were stealing everyone’s everywhere, all the time, and they still are right now. [...] Everything we do now lasts forever. Not because we want to remember it, but because we’re no longer allowed to forget. [...] The entire structure of the Internet has changed since 2013. The world’s biggest technology companies, good and bad for privacy, have reengineered the kind of protections that we experience, that you don’t even see, simply because they realized the government was sort of going in, undercover of darkness, and helping themselves to the buffet, without anybody noticing. Our laws have changed. Our international standards have changed. Before 2013, people knew that mass

¹⁶⁷³ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 138.

¹⁶⁷⁴ A study showed that post-Snowden, the opposition to government surveillance increased from 44% to 52% at federal level within a year. See in Maniam, S. [Shiva]. (19 February 2016). Americans feel the tensions between privacy and security concerns. <https://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns>.

¹⁶⁷⁵ USA, The White House. *Liberty and Security in a changing world*, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, (12 December 2013).

¹⁶⁷⁶ The Daily Show. (20 September 2019). *Interview with Edward Snowden. Edward Snowden - Permanent Record & Life as an Exiled NSA Whistleblower*. <https://www.youtube.com/watch?v=PArFP7ZJrtg>.

¹⁶⁷⁷ USA. Court of Appeals for the Ninth Circuit, Case 13-50572, (2 September 2020).

surveillance was possible, but it was kind of a conspiracy theory, because it was a suspicion. And that distance between suspicion and fact is everything in a democracy.¹⁶⁷⁸

Security policy remains relevant for measures taken to avert threats related to national security. An example of this is the “Protecting Americans’ Data from Foreign Surveillance Act”¹⁶⁷⁹, a bill proposed by US Senator Wyden, which would have linked national security issues to criticism of data trafficking. “Shady data brokers shouldn’t get rich selling Americans’ private data to foreign countries that could use it to threaten our national security”, Wyden said. The Act wanted to restrict the transfer of US citizens’ personal data to foreign countries. Under the Act, the US would have first created a list of countries to which data could be transferred. This limitation to “trustworthy” countries would have been similar to the efforts of the US with the JR Act¹⁶⁸⁰ to “pre-select” countries whose citizens are granted judicial redress in US courts. This would have threatened the “minimum of solidarity”, which is a principle of international law. Both Acts together highlight that, on the one hand, the US is concerned about China’s supremacy in digital transformation (especially through the rapid development of AI) and tries to wall off the domestic market from the influence of Chinese suppliers; on the other hand, US stakeholders are concerned about the extent of data trafficking by domestic companies which process personal data in a complex web of companies around the world. There are also fears that China, for its part, is becoming increasingly closed off for US companies through the Chinese data governance regime created since 2017, as confirmed by a US Senate hearing in which it was put on record that

since China’s standards regime is still taking shape, this is an area upon which the United States should press Beijing. The Chinese government should commit to revise regulations and standards that pressure U.S. companies to disclose source code, encryption keys, and other sensitive information such as proprietary product specifications in exchange for market access. Any government reviews should be conducted in a non-arbitrary and transparent manner and include international third-party accredited bodies. [...] The United States should build upon the alliance structures that have been successful since the end of World War II. Unilateral action will not only compel China to retaliate against U.S. companies; it will make Beijing double down on the very structural problems we want to address, feeding Beijing’s own narrative about cybersecurity governance.¹⁶⁸¹

In recent years, China introduced a variety of data protection measures.¹⁶⁸² Chinese law allows restrictions of data flows for national security purposes.¹⁶⁸³ According to European understanding, there is still a great deal of room for improvement as far as the protection of personal data against Chinese authorities’ access is concerned.¹⁶⁸⁴ Most of the Chinese population has a deep trust in the State and therefore might not consider it necessary to protect its personal data against governmental measures.¹⁶⁸⁵ Data

¹⁶⁷⁸ The Daily Show. (20 September 2019). *Interview with Edward Snowden. Edward Snowden - Permanent Record & Life as an Exiled NSA Whistleblower*. <https://www.youtube.com/watch?v=PArFP7ZJrtg>.

¹⁶⁷⁹ Wyden, R. [Ron]. (15 April 2021). *Wyden Releases Draft Legislation to Protect Americans’ Personal Data From Hostile Foreign Governments*. <https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments>.

¹⁶⁸⁰ See Chapter III, Section II.1.2.6.

¹⁶⁸¹ Sacks, S. [Samm]. (7 March 2019). *Testimony on “China: Challenges to U.S. Commerce, A Hearing Before the Senate Committee on Commerce, Science, and Transportation’s, Subcommittee on Security*.

<https://www.commerce.senate.gov/services/files/7109ED0E-7D00-4DDC-998E-B99B2D19449A>. P. 2–3.

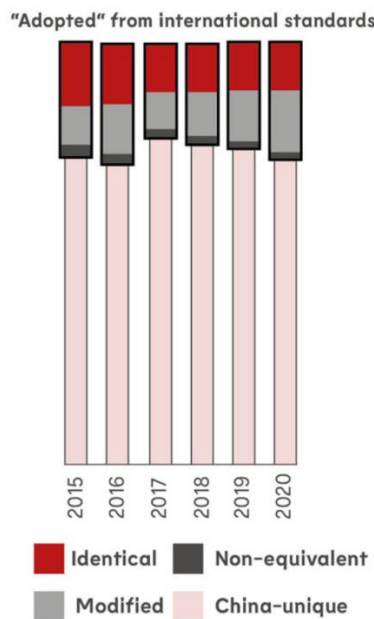
¹⁶⁸² See Chapter IV, Section IV.

¹⁶⁸³ See Chapter VIII, Section I.2.

¹⁶⁸⁴ See Chapter IX, Section III.3.

¹⁶⁸⁵ Statista GmbH. (17 January 2023). *Trust level in government in China 2016-2022*. <https://www.statista.com/statistics/1116013/china-trust-in-government-2020>.

protection in China tends to play a greater role in maintaining a common coexistence of citizens instead of safeguarding individual rights. Thus, awareness among the population of the need to protect their personal data is developing only slowly. On the other hand, the State has no great deal of interest in setting rules to protect its citizens' data whilst hereby limiting its own authority. This is different to the European perspective and has impacts on the approach by the Chinese regulatory stakeholders. While companies play an increasingly important role in the standard-setting processing China, the State ultimately retains authority. This enables standards to be used strategically to create competitive advantages for local companies over their international competitors. This can be illustrated using the following graphic as an example.



Source: Sinolytics GmbH, "Adoption rate of international standards remains low in China"¹⁶⁸⁶

In the European framework, the regulatory stakeholders have recognized that national security purposes must be defined more precisely. Art. 23(1)(a) GDPR allows restrictions for the protection of national security. This term is also found in Art. 4(2) TEU. Accordingly, national security is only threatened if an imminent damaging event calls into question the security of the State beyond collective or individual goods. National security is related but not identical to the concept of public security in Art. 23(1)(c) GDPR. The concept of public security is to be interpreted narrowly and is limited to particularly significant legal interests and elementary standards.¹⁶⁸⁷ There must be a "concrete danger" for these standards for regulations restricting data subjects' rights to be permissible. The legislator has some leeway in this respect; however, the fundamental goal of transparent data protection rules must not be jeopardized, and the principle of proportionality must be respected. This will in principle rule out a restrictive regulation even in the case of abstract risks and favors the interests of data subjects in those checks and balances.

¹⁶⁸⁶ Sinolytics GmbH. (11 July 2022). *Adoption rate of international standards remains low in China*. https://sinolytics.de/sinolytics_weekly.

¹⁶⁸⁷ Recital 73 of the GDPR mentions the "protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behavior under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes."

But not only pure security interests fall under a “national security policy” in a broader sense, but also a “public order policy.” States will also have an understandable interest in allowing the free TFPD only if they have “a clear and efficient framework with other countries that facilitates their timely access to data (related to a legitimate investigation) stored in that jurisdiction”¹⁶⁸⁸. Above¹⁶⁸⁹, however, significant weaknesses in the MLATs system have already been identified. As a result, there is “currently no comprehensive framework for how to successfully navigate cross-border jurisdictional disputes, especially those involving the digital economy. As the threat of cybercrime rises, there is an increasing need for clarity on these questions”¹⁶⁹⁰, particularly regarding government access to data domestic data stored in other nations.

A digital industrial policy within an economic policy “can reflect a view that data is a resource that needs to be made available first and foremost to national producers or suppliers. These approaches can be sector specific or apply to a range of data”¹⁶⁹¹. The interests of States diverge, with them acting as suppliers or as demanders on the global market, depending on the position of the national industry. Countries with export-oriented digital industrial policies have different interests than those that mainly import services or goods.

Those interests also diverge in terms of what States consider to be tradable goods or services.¹⁶⁹² Interests may also differ between States with a competitive digital industry and those with a monopolistic one, which may lead to conflicts in economic relations with other States. The more significant the market for digital services of a monopolistic States is for the export companies of a competitor country, the more acute this conflict of interest becomes.

In the last two decades of the 20th century, the relevance of a distinction between socialist-oriented States and capitalist-oriented States diminished; and equally, in the first two decades of the 21st century, the distinction between monopolistic States and competition-oriented States. These distinctions were replaced by a strengthening of nationally oriented governments, which was influenced by a combination of the developing digital economy, a lack of a harmonized level of data protection, the technological possibilities of domestic control over infrastructure, and the growth of extraterritorial regulations.

The latter was also driven by the GDPR. This regulation forced companies to comply with high data protection standards before expanding abroad. This led to concerns among regulatory stakeholders that national companies could even be forced to break the law because of conflicting obligations (e.g., government requests to produce personal data vs. prohibitions on disclosure for data protection reasons). The States involved would then not be able to fulfill their function of guaranteeing the rule of law.

One solution to this could be to act in the traditional way under international law by means of consensus building between States. However, since this approach is proceeding hesitantly, some States have recently tended toward a different solution, namely, to restrict their national market for imports of digital services or goods. The intention herewith is to protect the domestic digital industry and keep the competitive power of foreign providers with their technological advantage out of the national market. This

¹⁶⁸⁸ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

¹⁶⁸⁹ Chapter II, Section II.3.7.

¹⁶⁹⁰ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

¹⁶⁹¹ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 15.

¹⁶⁹² See also above the discussion on the application of GATS or GATT in Chapter V, Section III.

usually coincides with a “hoarding of data” to have the upper hand in the data economy in an international comparison.

In contrast to other interests, infrastructure policy interests had receded into the background during the worldwide spread of Internet access. However, in the context of emerging imbalances within the global digital economy and the increasing concentration on large providers, it has regained importance.

States may not only have an interest in restricting market access, but also in regulating competitors already participating in the domestic market. In this respect, economic policy and infrastructure policy are close. The rapid increase of data flows was accompanied by a rapid expansion of capacities for data processing, data transfer, and data storage. This influenced the States as stakeholders for the expansion of the network. The key issue was how to finance this expansion, for both public and private sectors. At the beginning of the Internet, this expansion was mostly driven by the public sector. In the last two decades, the provision of infrastructure has been left more to the market. This led to private telecommunications companies – which may have previously been state-owned or semi-state-owned – offering services in addition to their network connectivity services and starting to compete with large SPs such as Google. Since personal data are the new currency in many business models of those Internet companies, the use of personal data reinforced these effects, which in turn can lead to the formation of concentrated markets in platform competition. Therefore, governments are increasingly interested in considering interventions in competition policy, which could be justified if telecommunications companies have a dominant market position. This position could be regulated without the intervention of a State if the users of the services of the Internet companies would not “pay” with their personal data. On the one hand, this would presuppose that users were aware of their interests of the data subjects that could be used to influence the dynamics of this market through their changed user behavior. This awareness has indeed increased. However, so has the market power of companies. In addition, users are often unable to make an informed decision due to the non-transparent design of services, as the EUR 225 million fine against WhatsApp highlights.¹⁶⁹³ This led the Commission to initiate various proceedings against Google and to impose to Google a fine of EUR 1.49 billion.¹⁶⁹⁴

There are also State interests to establish a sovereign national Internet infrastructure: The Russian government has decided to control Internet traffic in its own country by allowing content to be filtered through government-controlled Internet nodes. Transition points into the global network can be restricted or shut down as needed, creating a *de facto* intranet for Russia. This is intended to protect against outside interference and that in the event of a disruption, such as a cyberattack, the Internet will still function on Russian territory. Russian ISPs have to create the technical conditions for this measure and place their servers under the supervision of a national public authority. “Russia has thus created the legal framework to shut down parts of the Internet and to more strongly control the kind of Internet that Russians can perceive in the country,” said Dutch data protection expert Joris van Hoboken.¹⁶⁹⁵ Similar approaches are also shown by other countries such as China, Iran, Vietnam, Cuba, and North Korea. After the Chinese

¹⁶⁹³ Irish Data Protection Commission. (2 September 2021). *Data Protection Commission announces decision in WhatsApp inquiry*. <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>.

¹⁶⁹⁴ European Commission. (20 March 2019). *Antitrust: Commission fines Google EUR 1.49 billion for abusive practices in online advertising*. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.

¹⁶⁹⁵ Hänel, L. [Lisa]. (2 May 2029). *Zensur im Netz: Russland folgt Chinas Beispiel*. *Deutsche Welle*. <https://www.dw.com/de/zensur-im-internet-nimmt-zu-russland-folgt-chinas-beispiel/a-48575267>.

government had already enforced a registration obligation for app stores¹⁶⁹⁶, it introduced an obligation for “Virtual Private Network Software” (VPN) clients, which critics call “the Great Firewall”.¹⁶⁹⁷ In the future, such software may only be offered with government permission. This contradicts the actual purpose of these VPN services, namely the encryption of Internet communication and the circumvention of possible censorship measures. With its “European Cloud”, the EU also shows intentions – albeit in a softened form – to detach itself from global developments and dependencies on large US providers.

Another area of regulatory stakeholder interests are technological policies. These naturally have a large overlap with infrastructural goals, but there are examples of domestic control that should be exemplarily mentioned here. China has intensified government surveillance by using – *inter alia* – DNA samples and biometric data such as facial and fingerprint recognition to monitor citizens across the country¹⁶⁹⁸ and by introducing the new “Social Credit System”¹⁶⁹⁹. The interest hereby is to create a system that evaluates the desired and undesired behavior of each citizen.

A legal policy is aligned with the other policies mentioned above and is thus a “bracket” around all interests of regulatory stakeholders, as Trakman/Walters/Zeller also underlined:

However, resort to public law measures to protect personal data internationally presupposes a consensus among states that is politically and economically fraught. States have different reasons for supporting or denying protections to data subjects, based on their localized ideological, economic and political policies. They include, among others, an ideology that support a free market in the exchange of information, a state’s reliance on revenue generated from data collectors and processors, and its public policy interest in, *inter alia*, national security, public health and social stability. They include the converse interest of governments not to constrain access to, or the use of, personal data in pursuit of revenues from data collectors and processors, notwithstanding the adverse human rights impact of that use upon data subjects.¹⁷⁰⁰

Measures of legal policy are “aimed at meeting different regulatory objectives, such as access to information for audit purposes. In this sense, requirements for data to be stored locally can be seen as the online equivalent of a longstanding practice in the offline world of ensuring that information is readily accessible to regulators. Such measures can be sector-specific, reflecting particular regulatory requirements and targeting specific data such as business accounts, telecoms or banking data”.¹⁷⁰¹ SAs also play a role at this

¹⁶⁹⁶ Benner, K. [Katie] and Wee, S.-L. [Sui-Lee]. (4 January 2017). Apple Removes New York Times Apps From Its Store in China. *The New York Times*. <https://www.nytimes.com/2017/01/04/business/media/new-york-times-apps-apple-china.html>.

¹⁶⁹⁷ Ye, J. [Josh]. (23 January 2017). China tightens Great Firewall by declaring unauthorized VPN services illegal. *South China Morning Post*. <https://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall>.

¹⁶⁹⁸ Lu, S. [Shen]. (10 December 2020). Facial Recognition Is Running Amok in China. The People Are Pushing Back. *VICE*. <https://www.vice.com/en/article/4adnyq/facial-recognition-is-running-amok-in-china-the-people-are-pushing-back>.

¹⁶⁹⁹ This system is a data-driven digital monitoring, recording, and rating system that ranks and rates individuals, public officials, companies, organizations, and associations. Bad behavior is disciplined and punished. The rating system goes back to the “Planning Draft for the Construction of a Social Credit System (2014-2020),” which was approved by the Chinese State Council on 14 June 2014. // PRC. *State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020)*, <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020>.

¹⁷⁰⁰ Trakman, L. [Leon] and Walters, R. [Robert] and Zeller, B. [Bruno]. (2019). Is Privacy and Personal Data Set to Become the New Intellectual Property?. *International Review of Intellectual Property and Competition Law*, 937–970, <http://dx.doi.org/10.2139/ssrn.3448959>. P. 963 f.

¹⁷⁰¹ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 15.

level. Further networking of SAs along the lines of the EU's EDPB could support this legislative function in an advisory and formative capacity.

2.2. International level

Forums of regulatory processes also exist at the international level. Clashes of interests are reflected on the one hand in forums for the self-organization of stakeholders, and on the other hand in intergovernmental organizations.

There is a “hybridization” of the law between national/supranational and international interests: The “internationalization of constitutional law” goes hand in hand with a “constitutionalizing international law”. National courts increasingly use international law sources when interpreting national law, also because international courts decide the same legal issues as the national courts. The CJEU for example recognized European fundamental rights as general legal principles early on.¹⁷⁰² In international law, the protection of fundamental rights plays a role, same as the question of possible international legal protection of governmental interests. The development of international human rights protection is one of the outstanding features of recent international law history. For a long time, the relationship between a State and its citizens was an internal matter for which international law did not contain any rules. This changed in the 19th century due to the emergence of rules which we now assign to the protection of human rights, and which were then standardized firstly in trade- and shipping contracts. Human rights can be differentiated according to their legal quality. Initially, all human rights are binding; this follows from the essentials of “law”.

As the hypothesis of this thesis is to present a binding regulatory instrument, forums of self-organization play a subordinate role, since these forums by their nature do not lead to binding decisions. Nevertheless, they are mentioned in this Section I.2.2 because they could play a role in a multi-stakeholder approach which also involves stakeholders of self-organization in the regulatory process towards a binding instrument. The most important self-organizational forums are the “International Chamber of Commerce” (ICC), the “International Telecommunication Users Group” (INTUG) and the “World Economic Forum” (WEF). The latter sees itself as a “Platform for Shaping the Future of Trade and Global Economic Interdependence” and made a significant contribution to the legal policy discussion in July 2020 with its “Data Free Flow with Trust (DFFT)”¹⁷⁰³ approach.

Most intergovernmental forums are united under the umbrella of the UN, which consists of the UN itself and its subordinate specialized agencies with subject-specific responsibilities, which together form the “UN system”. This includes the ITU, a specialized agency of the UN and the oldest international organization. As a forum for the global discourse on Internet Governance, the ITU has sought to re-establish itself with the “World Conferences on International Telecommunication” (WCIT). The “Internet Governance Forum” (IGF), mandated by the UN in 2006, is another relevant forum of interest, as it is more issue-specific with representatives of States, the network industry and civil society. The WTO, a “related organization” of the UN, has also published initiatives and regulatory proposals in the area of transborder data flow.¹⁷⁰⁴ The central fields of action of the UN are peacekeeping and conflict prevention, protection of human

¹⁷⁰² CJEU. Judgment of the Court of 12 November 1969, *Erich Stauder v City of Ulm – Sozialamt*, Case 29-69, ECLI:EU:C:1969:57, European Court reports 1969, 419–426.

¹⁷⁰³ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 12.

¹⁷⁰⁴ See Chapter V, Section III.

rights and fundamental freedoms, and promotion of international cooperation. These interwoven fields also include the task, arising from the fundamental rights approach, to support the norm-building process regarding a global right to data protection, which led to the standardization in Art. 17 ICCPR and Art. 12 UDHR. Convention 108 was the first legally binding convention on data protection. The T-PD of the COE is a committee of experts on data protection that acts in an advisory capacity and has developed a number of proposals on specific areas of data protection. During the discussions in March 2022 around a new EU-US agreement,¹⁷⁰⁵ it became known that within the OECD

countries have been working on a set of non-binding principles to govern government access to personal data, an issue that has become a key impediment to global data flows. [...] Those involved in the talks are confident that a breakthrough can be reached, especially in light of last week's EU-U.S. agreement. They eye a December timeline for the OECD's initiative to be up and running, though that deal would not override the transatlantic pact, but would instead operate in parallel to the deal done between Washington and Brussels. The Privacy Shield negotiations are legally and structurally separate from the OECD process, said Audrey Plonk, who is leading the initiative at the OECD. But I hope the agreement brings a breath of fresh air to the OECD negotiations.¹⁷⁰⁶

The responsibilities of these intergovernmental organizations were historically created based on various emerging problem areas. This created a complex structure of organizations, each calling for cooperation and regulation. Similarly, the task of keeping track of the overlapping interests of these organizations became more complicated, especially for cross-sectional problems such as the regulation of transborder data flow. The visions and missions of these organizations, which are informative for the presentation of the interests, are mostly derived from the preambles of the founding documents of those organizations.

One interest lies in a functioning trade, predominantly defined as the marketing of goods and services. In particular, the international order is required to satisfy the need of trade for legal certainty. This means that the international order must ensure both security of tenure and security of transaction. It must define rights of possession and rights of action and protect them from interference. In a single market, ensuring that stakeholders' agreements are enforceable is less problematic than when State borders are crossed, because the unity of the law and the State then falls apart and a State's monopoly on the use of force ends. This leads to a state of legal plurality. At the international level, the legal systems of the Member States to such organization then stand side by side on an equal footing. Another interest of intergovernmental organizations is thus to establish the "sovereign equality" recognized by international law. Since different legal systems naturally diverge, the international order has to regulate which Member State has jurisdiction and which law is applicable. The uncertainty in this, which has been explained above¹⁷⁰⁷, leads to higher transaction costs for the stakeholders of transborder data flows. This leads to an interest in harmonized rules to reduce legal uncertainties.

These organizations have an interest in ensuring that ratification processes are promising and as time-consuming as possible. This is difficult per se, as a large number of different stakeholders with different interests are involved in the process. Opposed to a fast procedure is also the interest of the Member States of an organization to obviously

¹⁷⁰⁵ See Chapter IX, Section II.1.

¹⁷⁰⁶ Manancourt, V. [Vincent] and Scott, M. [Mark]. (31 March 2022). The West's plan to keep global data flows alive. *Politico*. <https://www.politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/data-oecd-privacy-shield-national-security/amp>.

¹⁷⁰⁷ See Chapter VIII, Section III.

or covertly promote a Member State's own solutions. International organizations therefore seek a balance between, on the one hand, a solution that satisfies a large number of States but is time-consuming, and, on the other hand, a faster solution. The latter will be more difficult the more extensive the project of harmonization is and may then only reach an isolated regulation of a smaller and/or fragmentary scope of regulation.

Based on the ratification requirement of an international regulation, there is an interest that Member States can be persuaded to renounce their sovereignty at least to some extent. However, the probability of this only increases if the legal instrument in question provides a minimum level of participation in and protection of public goods for the affected Member States. This probability could be even higher if the contents of the instrument could form a basis of stability in such a way that a common ground between the interests of the Member States is found which does not pose a threat to the stability of the sovereignty of the Member State concerned.

Interests in transparency also play a role. As Weber noted, "the increase of transparency facilitates the decision-making processes for businesses that are considering how to handle transborder data flows"¹⁷⁰⁸; this also applies to the standardization processes of intergovernmental organizations, especially when this process implies a higher degree of loss of national sovereignty. This has also been acknowledged by the OECD, by pledging governments "to seek transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows"¹⁷⁰⁹.

For the success of a regulatory intervention at the international level, it would be important that its content is tailored to the needs of the addressees. Under a multi-stakeholder approach, this would require the participation of the relevant private and public stakeholders in the drafting and elaboration of the instrument to integrate the expertise of a wide range of stakeholders. However, this usually contradicts the interest of international organizations to negotiate only with Member States in such discussions and not to strain their limited human resources.

Moreover, after ratification, it would not be certain that an instrument would permanently fulfill the harmonization of law. Intergovernmental forums therefore have an interest in ensuring that such instrument does not thwart its original purpose through the natural evolution of case law and external circumstances. To this end, a regulatory instrument would have to be designed in such a way that it can be interpreted uniformly. Undefined legal terms, general clauses, or opening clauses could pose a danger to this. Particularly in data protection law, such terms and clauses could be defined too narrowly or too broadly due to a lack of sufficient legal expertise among all stakeholders. An extreme case of deficiencies in the content of a possible instrument could be gaps that arise because legal issues are not regulated at all, or because they are not covered by the scope of the instrument. Two burdens for intergovernmental organizations can then arise: On the one hand, Member States, in particular their judiciary, could tend to prefer the application of national law, at least for parts of the new instrument and temporarily. On the other hand, a comprehensive adaptation of the instrument to changed technological, economic, social or political circumstances (Chapter I) could become necessary, which could lead to a new ratification process with a considerable expenditure of resources. It is therefore likely to be in the interest of the

¹⁷⁰⁸ Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130. P. 121.

¹⁷⁰⁹ OECD. *Declaration on Transborder Data Flows*, https://www.oecd.org/document/32/0,3343,en_2649_34255_1888153_1_1_1_1,00.html, (11 April 1985).

intergovernmental organizations to draft of a regulatory measure that “enables[s] individuals and businesses to reach a high level of compliance at reasonable cost [...]”; regulators are called on to design a norm-setting that is more efficient”¹⁷¹⁰.

II. Arenas

The various stakeholder interests were described above. It is now to assign these interests to different arenas. To solve a lack of harmonization in this area of law, Farrell describes the possible approaches of an exertion of the above interests:

States may still try to solve collective action problems through unilateral action, through coordination among themselves, and through new forms of policy which mix public and private action. The second and third of these types of solution typically require negotiations which seek to harmonize forms of common good provision across arenas, or at least to ensure the compatibility of different solutions in different arenas. This layer of international negotiation provides new opportunities for actors in domestic arenas.¹⁷¹¹

Since the hypothesis of this thesis does not correspond to unilateral action, this Section II will focus on negotiations which seek to harmonize forms of common good provision across arenas. The aim will be to determine the arenas in such a way that the largest possible mass of the above-mentioned interests can be analyzed in each arena and that the sum of these arenas represents the largest possible geographical share of the global ecosystem of transborder data flows. The analysis of arenas is also important because “solutions in one particular arena of policy-making may be incompatible with the solution or broader regulatory mechanisms in another arena”.¹⁷¹² As Farrell notes, stakeholders and interests have been for example important on the way to Safe Harbor. One arena was the EU-US negotiations, the others were the development of domestic US law and supranational EU law at the time. Safe Harbor and Privacy Shield are annulled, and Farrell’s breakdown is based on a 2002 level. Nevertheless, the weighting of interests in this ecosystem has not changed much. Therefore, the approach of Farrell can still be followed. These arenas are potentially intersected: stakeholders who sought to influence developments in the first arena (EU-US negotiations) were motivated by goals that they were pursuing in the second (the domestic EU debate) or third (the domestic US debate) arena.

1. EU-US

The EU and the US are linked by the world’s most important trade relationship. Over 50% of the respective foreign investments in one region flow into the other. Consequently, the conditions for a transfer of personal data between EU and US are of an economic importance non-comparable to any other third country. Alex Greenstein, Director of the EU-US DPF at US Department of Commerce and head of the Privacy Shield for 4 years, commented on 14 July 2023:

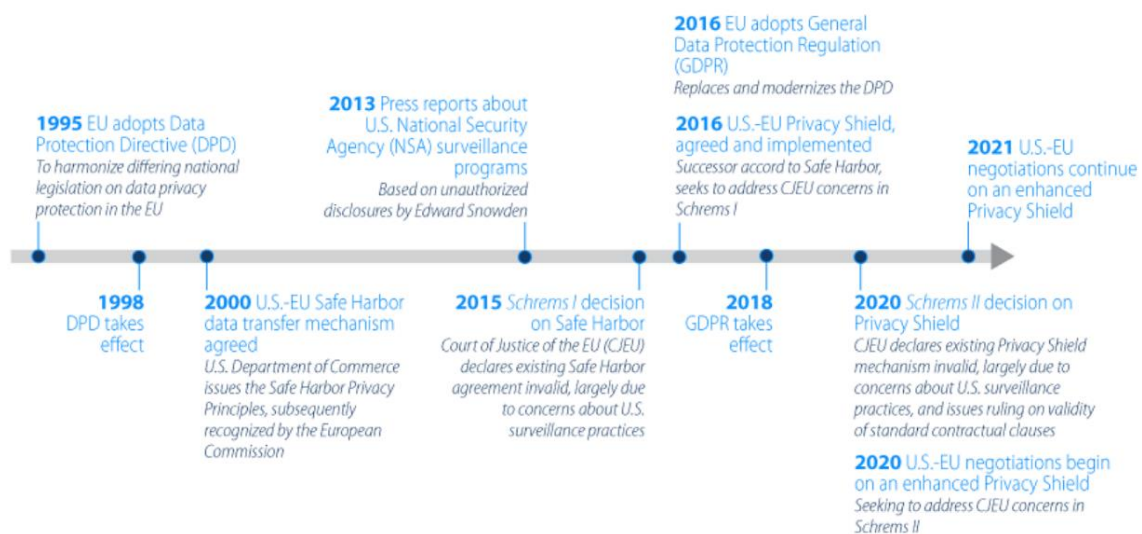
¹⁷¹⁰ Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130. P. 122.

¹⁷¹¹ Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US 'Safe Harbor' Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield. P. 101.

¹⁷¹² Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US 'Safe Harbor' Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield. P. 101.

The reason this is all so important is that data flows and the transfers of personal data are a key enabler for basically all elements of the transatlantic economic relationship. It's something so fundamental that it really underpins all elements of commerce and trade investment between the United States and Europe. [...] That's the biggest economic relationship in the world, and that's why this has been such a priority for the Biden administration and for the EU¹⁷¹³

Despite this economic importance for both sides, EU and US companies must overcome barriers in TFPD scenarios. These barriers are due to different levels of protection of personal data, which became evident through the provisions of Directive 95/46 for a transborder data flow, increased through *Schrems I* and *Schrems II*, and have not been fully resolved to date.



Source: US Congressional Research Service, "Timeline of Key Events for Commercial Transatlantic Data Flows"¹⁷¹⁴

Already during the existence of Safe Harbor, the US side placed emphasis on a free flow of data and believed that "regulation is inappropriate, given how swiftly e-commerce is evolving, and has instead sought to encourage self-regulation in areas such as privacy, in the belief that self-regulation would be more flexible and responsive"¹⁷¹⁵. European criticism about Safe Harbor argued, e.g., that the enforcement system of Safe Harbor "is weak", that the adequacy decision by the Commission "refers to a system that is not yet operational",¹⁷¹⁶ that the number of organizations self-certifying under Safe Harbor would be lower than expected, and that the whole process is based on a company's simple claim to adhere to certain standards, without compliance with them being guaranteed or verifiable.

These concerns continued regarding Privacy Shield. This agreement was criticized by the EDPS above all for its non-binding legal character.¹⁷¹⁷ The WP29 also expressed

¹⁷¹³ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*.

<https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

¹⁷¹⁴ USA, Congressional Research Service. *U.S.-EU Privacy Shield and Transatlantic Data Flows*, R46917, (22 September 2021). P. 2.

¹⁷¹⁵ Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US 'Safe Harbor' Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield. P. 105.

¹⁷¹⁶ WP29. *Opinion 4/2000 on the level of protection provided by the Safe Harbor Principles*, WP32, (16 May 2000). P. 7.

¹⁷¹⁷ EDPS. *Opinion on the EU-U.S. Privacy Shield draft adequacy decision*, Opinion 4/2016, https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf, (30 May 2016).

concerns and asked for various clarifications.¹⁷¹⁸ It further recommended that a review of the Commission's adequacy decision, as well as of the adequacy decisions issued for other third countries, should take place shortly after the GDPR enters into application.¹⁷¹⁹ On 25 May 2016, the Parliament concluded that the Commission should continue negotiations with the US in order to push for further improvements to the agreement in view of mayor shortcomings:

The access of the US authorities to data to be transferred under the Privacy Shield; the possible collection of data which, in some cases, does not meet the criteria of necessity and proportionality laid down in the ECHR; the proposed US ombudsman does not have the necessary independence and is not equipped with the appropriate powers for the effective exercise and enforcement of its tasks; the complexity of remedies, which the US authorities and the Commission should make user-friendly and efficient.¹⁷²⁰

Shortly after, the WP29 issued a press release and commented on Privacy Shield's adoption by the Commission that "a number of these concerns remain regarding both the commercial aspects and the access by U.S. public authorities to data transferred from the EU".¹⁷²¹ On 16 September 2016, Privacy advocacy group Digital Rights Ireland also challenged the Privacy Shield agreement.¹⁷²² A Commission spokesman replied that the Commission is "convinced that the Privacy Shield will live up to the requirements".¹⁷²³ LIBE also expressed criticism on 23 March 2017.¹⁷²⁴ LIBE was concerned about, inter alia, that there is no reliable definition of mass surveillance, that the right of the data subjects cannot be enforced at all or hardly, and that the proposed Ombudsman lacks independence.

In his annual report for 2019, the "US Trade Representative" (USTR), alerted by the Privacy Shield being challenged in the EU, criticized the EU for barriers in the area of digital trade, which arose through the GDPR:

The United States remains concerned, that the implementation and administration of the GDPR create disproportionate barriers to trade, not only for the United States, but for all countries outside of the EU. Although the United States has received a determination of partial adequacy from the EU [for information on the European Union-United States Privacy Shield framework, see below], there are many other countries, including India, Japan, and Korea, that have expressed interest in obtaining an adequacy determination to facilitate the exchange of data with the EU. [...] The EU has so far found only a handful of countries to provide adequate data protection under EU law, which means that suppliers in the large majority of EU trading partners must rely on other arrangements or criteria to transfer data with suppliers in the EU. Moreover,

¹⁷¹⁸ "The WP29 also concludes that onward transfers of EU personal data are insufficiently framed, especially regarding their scope, the limitation of their purpose and the guarantees applying to transfers to Agents. [...] As regards the access to Privacy Shield data by law enforcement, especially to foreseeability of the legislation is a concern, due to the extensive and complex nature of the U.S. law enforcement system at both Federal and state level, and the limited information included in the adequacy decision." See WP29. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, WP 238, (13 April 2016). P. 3, 57.

¹⁷¹⁹ WP29. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, WP 238, (13 April 2016). P. 58.

¹⁷²⁰ European Parliament. (26 May 2016). *Geplanter EU-US-Datenschutzschild verbesserungswürdig*.

<http://www.europarl.europa.eu/news/de/press-room/20160524IPR28820/geplanter-eu-us-datenschutzschild-verbesserungswurdig>.

¹⁷²¹ WP29. *Statement on the decision of the European Commission on the EU-U.S. Privacy Shield*,

https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf, (26 July 2016).

¹⁷²² CJEU. *Digital Rights Ireland v Commission*, case T-670/16, OJ C 410/26, ECLI:EU:T:2017:838, (7 November 2016).

¹⁷²³ Fioretti, J. [Julia] and Volz, D. [Dustin]. (26 October 2016). Privacy group launches legal challenge against EU-U.S. data pact. *Reuters*. <https://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK>.

¹⁷²⁴ European Parliament. *Adequacy of the protection afforded by the EU-US Privacy Shield*, 2016/3018(RSP), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0131_EN.html, (6 April 2017).

legal challenges in the EU continue to create uncertainty around the transfer of data for U.S. and other foreign companies¹⁷²⁵

After cautious assessments in the second half of 2020 because the new US administration was not yet in place,¹⁷²⁶ and the EU's first formalized institutional message after the US election 2020 to its "natural partner" to initiate a dialogue on a new transatlantic agenda based on shared essential values¹⁷²⁷, the EU and the US set out, following the election of POTUS Biden, a new "Transatlantic Agenda"¹⁷²⁸. The Commission focused herein on those areas in which the US and European interests "converge" and the collective leverage can best be used, at the same time also those in which "our global leadership is necessary". One of these areas also includes cooperation with the US on "technology, trade and standards". The agenda includes detailed proposals such as the development of a joint transatlantic approach to the protection of critical technologies taking into account global economic and security concerns, including 5G, AI, and standards for free flow of data, the establishment of a US-EU council on trade and technology, and a transatlantic dialogue via digital platforms and BigTech.¹⁷²⁹ The Commission also spoke of facilitating bilateral trade and deepening cooperation in the areas of regulation and standardization and, if necessary, systematically coordinating positions in international standardization bodies. Section 4 on "Working together on technology, trade and standards" contains considerations that also concern transborder data flows: "We must also openly discuss diverging views on data governance and see how these can be overcome constructively. The EU and the US should intensify their cooperation at bilateral and multilateral level to promote regulatory convergence and facilitate free data flow with trust on the basis of high standards and safeguards."¹⁷³⁰

In 2021, it became known that the new Biden administration "is seeking - in the form of a high-level political agreement with European Commission President Ursula von der Leyen during the upcoming EU-U.S. summit - [a deal which] would lay the groundwork for a new transatlantic data transfer deal"¹⁷³¹. The aim was "to secure overarching commitments to fast-track negotiations, which have so far struggled to overcome legal questions about how Washington can better protect EU citizens' privacy rights".¹⁷³² Preparatory discussions to this EU-US summit led to a joint statement by EU Commissioner for Justice Didier Reynders and US Secretary of Commerce Gina Raimondo, in which they noted that

these negotiations underscore our shared commitment to privacy, data protection and the rule of law and our mutual recognition of the importance of transatlantic data flows

¹⁷²⁵ USA. *Trade Representative. 2019 National Trade Estimate Report on Foreign Trade Barriers*, https://ustr.gov/sites/default/files/2019_National_Trade_Estimate_Report.pdf, (15 March 2019). P. 207 ff.

¹⁷²⁶ Chee, F. Y. (Foo Yun]. (4 December 2020). Not any time soon, says EU privacy watchdog. *Reuters*. <https://www.reuters.com/article/eu-privacy-idUSKBN28E2JQ>.

¹⁷²⁷ "Our shared values of human dignity, individual rights and democratic principles make us natural partners to harness rapid technological change and face the challenges of rival systems of digital governance." European Commission. *A new EU-US agenda for global change*, JOIN(2020) 22 final, (2 December 2020). P. 5

¹⁷²⁸ European Commission. *A new EU-US agenda for global change*, JOIN(2020) 22 final, (2 December 2020).

¹⁷²⁹ "We must also openly discuss diverging views on data governance and see how these can be overcome constructively. The EU and the US should intensify their cooperation at bilateral and multilateral level to promote regulatory convergence and facilitate free data flow with trust on the basis of high standards and safeguards. [...] [The EU] "will propose a new transatlantic dialogue on the responsibility of online platforms, which would set the blueprint for other democracies facing the same challenges. We should also work closer together to further strengthen cooperation between competent authorities for antitrust enforcement in digital markets." European Commission. *A new EU-US agenda for global change*, JOIN(2020) 22 final, (2 December 2020). P. 5–6.

¹⁷³⁰ European Commission. *A new EU-US agenda for global change*, JOIN(2020) 22 final, (2 December 2020). P. 5–6.

¹⁷³¹ Scott, M. [Mark]. (2 June 2021). Biden seeks high-level data deal to repair EU-US digital ties. *Reuters*. <https://www.politico.eu/article/joe-biden-data-transfers-privacy-shield-eu-transatlantic>.

¹⁷³² Scott, M. [Mark]. (2 June 2021). Biden seeks high-level data deal to repair EU-US digital ties. *Reuters*. <https://www.politico.eu/article/joe-biden-data-transfers-privacy-shield-eu-transatlantic>.

to our respective citizens, economies, and societies. Our partnership on facilitating trusted data flows will support economic recovery after the global pandemic, to the benefit of citizens and businesses on both sides of the Atlantic.¹⁷³³

The joint statement after the EU-US Summit 2021 also contains a passage concerning transborder data flows:

We commit to work together to ensure safe, secure, and trusted cross-border data flows that protect consumers and enhance privacy protections, while enabling Transatlantic commerce. To this end, we plan to continue to work together to strengthen legal certainty in Transatlantic flows of personal data. We also commit to continue cooperation on consumer protection and access to electronic evidence in criminal matters.¹⁷³⁴

At this Summit, a forum was also created, the “EU-US Trade and Technology Council” (TTC), whose task is “to coordinate approaches to key global trade, economic and technology issues, and to deepen transatlantic trade and economic relations based on shared democratic values”¹⁷³⁵. This forum is not intended purely as a dialog forum, but to involve a wide range of stakeholders, and therefore corresponds to a multi-stakeholder approach.

The statements until end-2021 emphasized the recognition of the importance of a free flow of data and legal certainty within TFPD but left open concrete proposals for solutions. European Commission Vice President Věra Jourová asserted that, “on the commercial side, we don’t see such a big issue [...] but of course, there is the issue of access to data from the national security agencies [...] a legally-binding rule would be very useful, I would even say necessary.”¹⁷³⁶ European Commissioner for Justice Didier Reynders said a deal “would have to acknowledge the enforcement of an individual’s rights, giving Europeans’ administrative redress to a U.S. court for data breaches, [...] the goal was to avoid “Schrems III”.¹⁷³⁷ However, this demand for effective judicial protection, which is based on Art. 47 of the Charter, can hardly be implemented without a change in US law, for which there might be little chance in US Congress.¹⁷³⁸

The EU and the US are nevertheless at least in ongoing talks to resolve the “legal limbo facing thousands of companies, which is not ended by the separate agreement on SCCs [SDPC]”¹⁷³⁹. At the time of closing the research for this thesis, this “limbo” seems to have been advanced by a “preliminary deal” concluded in March 2022. The Commission President’s commented that EU and US “found an agreement in principle on a new framework for transatlantic data flows”, which will “enable predictable and trustworthy

¹⁷³³ European Commission. *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo*, https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443, (25 March 2021).

¹⁷³⁴ Council of the EU. *EU-US summit statement: Towards a renewed Transatlantic partnership*. <https://www.consilium.europa.eu/media/50758/eu-us-summit-joint-statement-15-june-final-final.pdf>. (15 June 2021). Para. 20.

¹⁷³⁵ European Commission. *EU-US Trade and Technology Council: Commission launches consultation platform for stakeholder’s involvement to shape transatlantic cooperation*, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_5308, (18 October 2021).

¹⁷³⁶ USA, Congressional Research Service. *U.S.-EU Privacy Shield and Transatlantic Data Flows*, R46917, (22 September 2021). P. 17.

¹⁷³⁷ Chee, F. Y. (Foo Yun). (2 June 2021). More safeguards in revamped EU data transfer tools, EU justice chief says. *Reuters*. <https://www.reuters.com/technology/more-safeguards-revamped-eu-data-transfer-tools-eu-justice-chief-says-2021-06-02>.

¹⁷³⁸ To be analyzed below Chapter IX, Section II.2.

¹⁷³⁹ Chee, F. Y. (Foo Yun). (2 June 2021). More safeguards in revamped EU data transfer tools, EU justice chief says. *Reuters*. <https://www.reuters.com/technology/more-safeguards-revamped-eu-data-transfer-tools-eu-justice-chief-says-2021-06-02>.

EU-US data flows, balancing security, the right to privacy and data protection”.¹⁷⁴⁰ This agreement is, according to Mr. Wiewiórowski, the EDPS, “the only piece of the puzzle that is missing” for legal deals underpinning bilateral data flows among most members of the G-7.¹⁷⁴¹ This new “EU-US Data Privacy Framework” (EU-US DPF) will “enable predictable and trustworthy data flows between the EU and U.S., safeguarding privacy and civil liberties”¹⁷⁴². It remains to be seen¹⁷⁴³ whether this framework will then fulfill the essential guarantees of the European framework to actually prevent a “*Schrems III*”. This is because NOYB has already announced its intention to take legal action against a new adequacy decision by the Commission based on this EU-US DPF, should the Commission accept the effects of the US “Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities” [EO 14086] on the US framework as ensuring an essentially equivalent level of data protection.¹⁷⁴⁴

Of importance is also how the EU and US position themselves in relation to other countries. In the EU-US agenda for global change, both have jointly stated that

the EU and the US need to join forces as tech-allies to shape technologies, their use and their regulatory environment. Using our combined influence, a transatlantic technology space should form the backbone of a wider coalition of like-minded democracies with a shared vision on tech governance and a shared commitment to defend it. To deliver on this, the EU must stay course for its own tech goals and ambitions as part of Europe’s digital decade.¹⁷⁴⁵

2. US

On the US side, two developments are currently taking place that influence the second arena, which is the domestic debate on data protection within the US. One is the direct reaction to the EU-US arena, the other is the further development of US State legislation and US federal legislation.

The developments in the US arena, as a direct reaction to the EU-US arena, date back to 1998. At that time, Directive 95/46 was noticed also in the US. From then on, a discussion developed about the right approach to data protection in the US. Stakeholders preferred either formal legislation or self-regulation. Marc Rotenberg, former director of EPIC, was back then one of the representatives who spoke out against self-regulation: “The self-regulatory approach that has been offered as an alternative to strong legal and technical protections is not doing very well. Public support for privacy legislation has grown during the time that self-regulatory policies have been pursued.”¹⁷⁴⁶

It is worth noting that even then Rotenberg pointed already to a looming isolation of the US and negative implications for transborder data flow:

¹⁷⁴⁰ Van der Leyen, U. [Ursula]. @vonderleyen. (25 March 2022). *Pleased that we found an agreement in principle on a new framework for transatlantic data flows. It will enable predictable and trustworthy EU-US data flows, balancing security, the right to privacy and data protection. This is another step in strengthening our partnership.* <https://twitter.com/vonderleyen/status/1507286853224914949>.

¹⁷⁴¹ Stupp, C. [Catherine]. (9 September 2022). *G-7 Privacy Regulators Aim To Ease Turbulent International Data Flows.* The Wall Street Journal. <https://www.wsj.com/articles/g-7-privacy-regulators-aim-to-ease-turbulent-international-data-flows-11662730512>.

¹⁷⁴² Manancourt, V. [Vincent]. (25 March 2022). *EU, US strike preliminary deal to unlock transatlantic data flows.* Politico. <https://www.politico.eu/article/eu-us-strike-preliminary-deal-to-unlock-transatlantic-data-flows>.

¹⁷⁴³ To be discussed below in Chapter IX, Section III.3.

¹⁷⁴⁴ NOYB. (7 October 2022). *New US Executive Order unlikely to satisfy EU Law.* <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>.

¹⁷⁴⁵ European Commission. *A new EU-US agenda for global change*, JOIN(2020) 22 final, (2 December 2020). P. 5.

¹⁷⁴⁶ EPIC. (7 May 1998). *Testimony and Statement for the Record of Marc Rotenberg on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives.* <https://epic.org/privacy/intl/rotenberg-eu-testimony-598.html>.

Other countries are following the European approach and adopting new laws and new technical measures to protect privacy. The United States is becoming increasingly isolated in the global debate over privacy protection. Europe is committed to the enforcement of the Directive [95/46]. Failure by the United States to address this issue will have specific economic consequences for US firms and transborder data flows.¹⁷⁴⁷

Business stakeholders were on the other side of the debate. They criticized that data protection standards could represent a trade barrier that could have an impact on EU-US e-commerce.

The further development of US federal legislation has two main options. One is a statutory solution, which would require US Congressional approval. Recently, ADPPA was formally introduced in the US House of Representatives as one of several legislative proposals to address this issue.¹⁷⁴⁸ The other is a non-statutory solution, where such approval is not required; this category includes the US implementation of the EU-US DPF. The question is how these objectives might be implemented in the US framework. Sean Heather, Senior Vice President of Regulatory Affairs at the US Chamber of Commerce, stated in February 2022 that “what we’re working to negotiate right now is something that threads the needle between what the European Court of Justice requires under European human rights law, and also sort of what is possible under the U.S. Constitution, and also what is advisable given the national security commitments that the United States has”¹⁷⁴⁹. This understandably provides the balance that would need to be maintained for the implementation process in the US. If, and the way in which these two options are implemented, directly affects the question of whether the requirements set by *Schrems I / II* for an “essentially equivalent level of data protection” could be met. This will be discussed further within the comparative analysis of the “essential guarantees” in this Chapter IX, Section III.3.

At US State level, there have been comprehensive legislative approaches to data protection in recent years. Several other States have comprehensive data protection initiatives – that include opt-in approaches for consent, private right of action, and other provisions for strong protection – in committee, including Massachusetts (SD 1762, HD 2664), New York (A 680), and New Jersey (A 505). Fourteen of twenty proposed State laws nevertheless appear to be a “Virginia-esque” bill, approaching the level of protection standardized by the VCDPA, but do not exceed it:

¹⁷⁴⁷ EPIC. (7 May 1998). *Testimony and Statement for the Record of Marc Rotenberg on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives*. <https://epic.org/privacy/intl/rotenberg-eu-testimony-598.html>.

¹⁷⁴⁸ See also Chapter III, Section II.1.2.8.

¹⁷⁴⁹ Heather, S. [Sean]. (28 February 2022). *Hope Springs Eternal? Assessing the State of U.S.-EU Digital Cooperation*. State of the Net conference in Washington, D.C. <https://www.stateofthenet.org/sotn-22>.

● Virginia-based or Weaker Bill ● Other Privacy Bill



Source: The Markup, “States with proposals for privacy bills, by type”¹⁷⁵⁰

None of these proposals achieve the level of protection established by the CPRA, and thus not the level of protection of the European framework. Should most of the US States follow the Virginia model, then this could “really hamstring federal lawmakers’ ability to do anything stronger, which is really concerning considering how weak [that model] is”¹⁷⁵¹. Moreover, a “small handful of bills that have not adhered to two key industry demands – that companies can’t be sued for violations and consumers would have to opt out of rather than into tracking – have quickly died in committee or been rewritten”¹⁷⁵².

3. EU

European legislators’ long-term aim with the GDPR was also to set a “gold standard” that influences the international development of data protection law and political processes in other countries.¹⁷⁵³ An IAPP-EY Privacy Governance report found that more than half (51%) of 473 MNEs rate themselves very or fully compliant with the GDPR, versus 41% for CCPA and 21% for Brazil’s *Lei Geral de Proteção de Dados* (LGPD).¹⁷⁵⁴ The GDPR is thus influencing regulators in third countries.

Nevertheless, the justification of such gold standard depends first on elements being inherent in the GDPR; second, on the adaptability of the GDPR to external factors of the four dimensions mentioned above¹⁷⁵⁵; third, on the promotion of the European approach through the participation of the EU in international agreements on data protection; and

¹⁷⁵⁰ Feathers, T. [Todd]. (15 April 2021). *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*. <https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious>.

¹⁷⁵¹ Feathers, T. [Todd]. (15 April 2021). *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*. <https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious>.

¹⁷⁵² Nicodemus, A. [Aaron]. (5 May 2021). Private right of action proving problematic for state privacy laws. *Compliance Week*. <https://www.complianceweek.com/data-privacy/private-right-of-action-proving-problematic-for-state-privacy-laws/30343.article>. // Feathers, T. [Todd]. (15 April 2021). *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*. <https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious>.

¹⁷⁵³ EDPS. (1 April 2016). *The EU GDPR as a clarion call for a new global digital gold standard*. https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_de.

¹⁷⁵⁴ LaLonde, B. [Brandon] and Thompson, M. [Mark] and Kanthasamy, S. [Saz]. (2021). *IAPP-EY Annual Privacy Governance Report 2021*. <https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2021>. P. 26.

¹⁷⁵⁵ Chapter I, Section I.

fourth, on the recognition of the Union’s “essential guarantees” in other laws at global level. This Section II.3 will cover these first three points since essential guarantees will be dealt with in Section III.3.

The GDPR is the result of the Union’s efforts to provide a uniform normative basis for data protection. It stood at the end of a laborious process that had to find compromise between multi-dimensional conflicts of interest. Participation to find such compromise and to improve the GDPR is high, through a Commission’s report,¹⁷⁵⁶ statements by Member States¹⁷⁵⁷ and the Council¹⁷⁵⁸, as well as numerous reactions from civil society associations. Digital development has always been faster than legislation and will naturally remain so. The European internal market therefore needs constant regulatory progress to meet objectives of improvement. Digitization is influenced by data protection legislation. The improvement of the GDPR must therefore constantly be measured against the objectives of digitization. It is therefore not surprising that a few years after the GDPR came into force, calls revolved to adjust the GDPR as quickly as possible to the latest developments in the area of digitization.

The GDPR treats all those responsible for data processing activities and all personal data basically the same. Given the data explosion of the Internet age, this approach tends to lead to overregulation of broad areas of economic and private life. One point of criticism, raised by Roßnagel / Geminn¹⁷⁵⁹, was therefore that the GDPR is too risk-neutral regarding data protection principles, the requirements for the lawfulness of processing, and the rights of data subjects. They argued that neutrality may make sense elsewhere, but not in the case of new technologies such as Big Data and AI. If too strictly risk-neutral, this could lead to “allotment gardeners or sports clubs being subject to the same data protection requirements as large global corporations, which have far greater data processing power and thus naturally pose a higher risk to the fundamental rights of individuals”¹⁷⁶⁰.

Because of the GDPR’s accountability principle, those responsible for the processing of personal data must also be able to prove at any time that their data processing activities comply with the provisions of the GDPR. This principle applies to all sizes of those responsible, be them car service stations or large technology groups. The associated documentation effort can be a considerable additional burden, especially for SMEs. This burden could be even increased by *Schrems II*, which now imposes on those responsible a complex TIA¹⁷⁶¹ that must be carried out before an export of personal data to third countries.

Another principle that can cause problems if interpreted too narrowly is that of purpose limitation. Data processings can conflict with a narrow purpose limitation, since at the time of the collection of personal data, it may not be possible to fully determine to which purposes such data processings will ultimately lead to.

¹⁷⁵⁶ European Commission. *Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock*, COM(2019) 374 final, (24 July 2019).

¹⁷⁵⁷ Council of the EU. *Preparation of the Council position on the evaluation and review of the GDPR – Comments from Member States*, ST 12756/1/19, <https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf>, (9 October 2019).

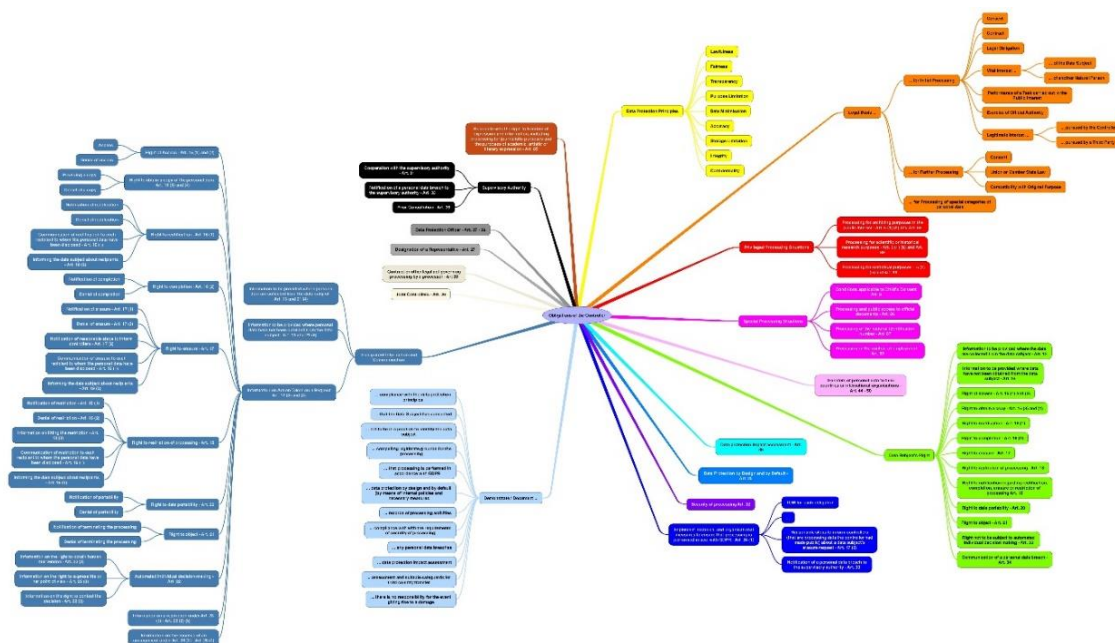
¹⁷⁵⁸ Council of the EU. *Council position and findings on the application of the General Data Protection Regulation (GDPR)*, ST 14994/2/19, Rev. 2, <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/en/pdf>, (15 January 2020).

¹⁷⁵⁹ Roßnagel, A. [Alexander] and Geminn, C. [Christian]. (2020). *Datenschutz-Grundverordnung verbessern*. Nomos. P. 153

¹⁷⁶⁰ Roßnagel, A. [Alexander] and Geminn, C. [Christian]. (2020). *Datenschutz-Grundverordnung verbessern*. Nomos. P. 153

¹⁷⁶¹ See Chapter II, Section II.3.4.4.g.

Another point of criticism was that the GDPR may inhibit innovation. The GDPR's prohibition principle entails that the processing of personal data is prohibited unless those responsible can invoke an element of permission. This means, first, that personal data may not be processed "by default". This general contradiction to the general freedom of action is intended by data protection law; on the one hand, to fulfill the notice and warning function of the GDPR, and on the other hand, to follow the preventive character of the GDPR. This regulatory concept is in principle hostile to processing activities. Admittedly, there are permissive elements for many data processing scenarios, which relativizes the rigor of the prohibition principle. Naturally, however, it makes a difference whether a processing activity is fundamentally permitted or fundamentally prohibited. Those responsible must also provide reasons for the data processing vis-à-vis the data subjects as well as the SAs. This leads to numerous obligations, which Veil called a "hypertrophy of obligations", that "do not provide a favorable environment for a data processor to promote data processing activities".¹⁷⁶²



Source: Veil, W. [Winfried], "GDPR: 68 Obligations of the Controller"¹⁷⁶³

The Union's – to put it bluntly – “no data are the best data” approach can ultimately lead to difficulties when using systems driven by technological innovations that have only been ready for the market in recent years and that deliver the best results when they have the largest possible amount of data available. Exemplarily, research-intensive areas may not solely rely on anonymized data but need to process pseudonymized data to meet their research objectives.

An unintended deterrent effect of the GDPR can also occur, which are the so-called “chilling effects”. Those describe certain effects of State action, which lead to citizens no longer making use of their fundamental rights, although they would be entitled to do so. One of the goals of data protection law is to prevent such chilling effects. Individuals should be able to exercise all their fundamental rights as freely as possible, as long as they do not exceed the limits of a prohibition or violate the rights of other citizens. In practice, however, uncertainty about the scope of the GDPR is noticeable among both

¹⁷⁶² Veil, W. [Winfried]. (17 February 2018). *GDPR: 68 Obligations of the Controller*. <https://www.flickr.com/photos/winfried-veil/25437610017>.

¹⁷⁶³ Veil, W. [Winfried]. (17 February 2018). *GDPR: 68 Obligations of the Controller*. <https://www.flickr.com/photos/winfried-veil/25437610017>.

individuals and companies. In its strongest form, chilling effects can lead to a preference not to access personal data at all in the face of such uncertainty. Incorrect / incomplete data could be collected, and sporadic datasets hardly ever shared or merged with other data. Current technologies such as Industry 4.0, AI and Big Data analytics could then not be fed with sufficient data and the mastering or even further developing of such technologies could then become more difficult. The impact on business and innovation should therefore not be underestimated.

Moreover, it is still not clear whether another objective of the GDPR, full harmonization, can be maintained. For the Commission, harmonization remains central.¹⁷⁶⁴ However, this was *de facto* abandoned by 70 opening clauses.

As mentioned above¹⁷⁶⁵, European stakeholders still need to ensure the cooperation between the European SAs and the “one-stop-shop” mechanism to be more solid. Although the CEF and the EDPB’s interpretation of Art. 60 GDPR could bring improvements in this respect, it remains to be seen if the “one-stop-shop” mechanism will represent a continuing deficit. The EDPS therefore shared “views of those who believe we still do not see sufficient enforcement, particularly against Big Tech”.¹⁷⁶⁶ European Commission Vice-President Věra Jourová therefore presented three scenarios for improvement:

- Changing nothing: counting on the fact the cooperation in the context of the one-stop show will improve with time, as there are signs of improvement already;
- Revolution: Reopening the file to clarify certain concepts aligned with the EDPB’s guidelines [Guidelines 02/2022 on the application of Article 60 GDPR] and to centralize enforcement;
- Targeted improvements: Administrative procedures would be streamlined as far as possible under EU law, DPAs would collaborate with other regulators, such as competition authorities, based on the one-stop-shop experience, and the EDPB would have a more decisive role with a stronger secretariat.¹⁷⁶⁷

Another issue related to SAs is whether the various national SAs within the European framework might go too far with their interpretation of *Schrems II* and the related EDPB and EDPS guidelines. Various SA decisions¹⁷⁶⁸ around the use of Google Analytics underscore how far the SAs go in some cases with their assessment of sufficient supplementary measures. The French SA, e.g., found that

these transfers are illegal and orders a French website manager to comply with the GDPR and, if necessary, to stop using this service under the current conditions. [...]. Although Google has adopted supplementary measures to regulate data transfers in the context of the Google Analytics functionality, these are not sufficient to exclude the accessibility of this data for US intelligence services. There is therefore a risk for French website users who use this service and whose data are exported. The CNIL notes that the data of Internet users is thus transferred to the United States in violation of Articles

¹⁷⁶⁴ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 17.

¹⁷⁶⁵ Chapter IX, Section I.1.4

¹⁷⁶⁶ Bertuzzi, L. [Luca]. (28 June 2022). *10 years after: The EU’s ‘crunch time’ on GDPR enforcement*. <https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement>.

¹⁷⁶⁷ Bertuzzi, L. [Luca]. (28 June 2022). *10 years after: The EU’s ‘crunch time’ on GDPR enforcement*. <https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement>.

¹⁷⁶⁸ See Chapter II, Section II.3.4.4.g.

44 et seq. of the GDPR. The CNIL therefore ordered to the website manager to bring this processing into compliance with the GDPR, if necessary, by ceasing to use the Google Analytics functionality (under the current conditions) or by using a tool that does not involve a transfer outside the EU/EEA. The website operator in question has one month to comply.¹⁷⁶⁹

The integration of Google Analytics, as it has been done by approximately 73% of the users of web analytics technologies,¹⁷⁷⁰ could therefore be severely impaired. Another ruling¹⁷⁷¹ from Germany shows that, after *Schrems II*, there will probably be further court rulings that classify the integration of web services that involve the transfer of personal data (IP addresses in this particular case) to the US as not conforming to the GDPR. The IAPP therefore noted that there is a trend “toward broader EU definitions of when data may not be processed by entities connected with third countries, including but not limited to the United States”¹⁷⁷².

Data protection rules for transborder transfers usually concern the exchange of data between (law enforcement) authorities of two or more Parties, or the transfer between private organizations. The interaction between the CCC, the LED and the GDPR becomes complex when it comes to the production of data by SPs.¹⁷⁷³ Another issue in the EU arena is therefore that increased regulation in data protection law creates considerable difficulties in differentiating between legislations, which entails time-consuming considerations even for subject-matter experts. This has even more been increased in complexity by the Commission’s Digital Single Market Strategy¹⁷⁷⁴ and Data Strategy¹⁷⁷⁵:

¹⁷⁶⁹ *Commission Nationale de l’Informatique et des Libertés*. (10 February 2022). *Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply*. <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>

¹⁷⁷⁰ “Google dominated the web analytics industry in 2021, with three of its web analytics technologies maintaining the top three positions in the global market. Google Analytics was first with a market share of 30 percent, followed by Google Universal Analytics and Google Global Site Tag who had market shares of 24 and 20 percent, respectively. When all three technologies were combined, Google maintained more than 70 percent of the total market share.” Statista GmbH. (13 September 2022). *Web analytics software market share worldwide 2022*. <https://www.statista.com/statistics/1258557/web-analytics-market-share-technology-worldwide>.

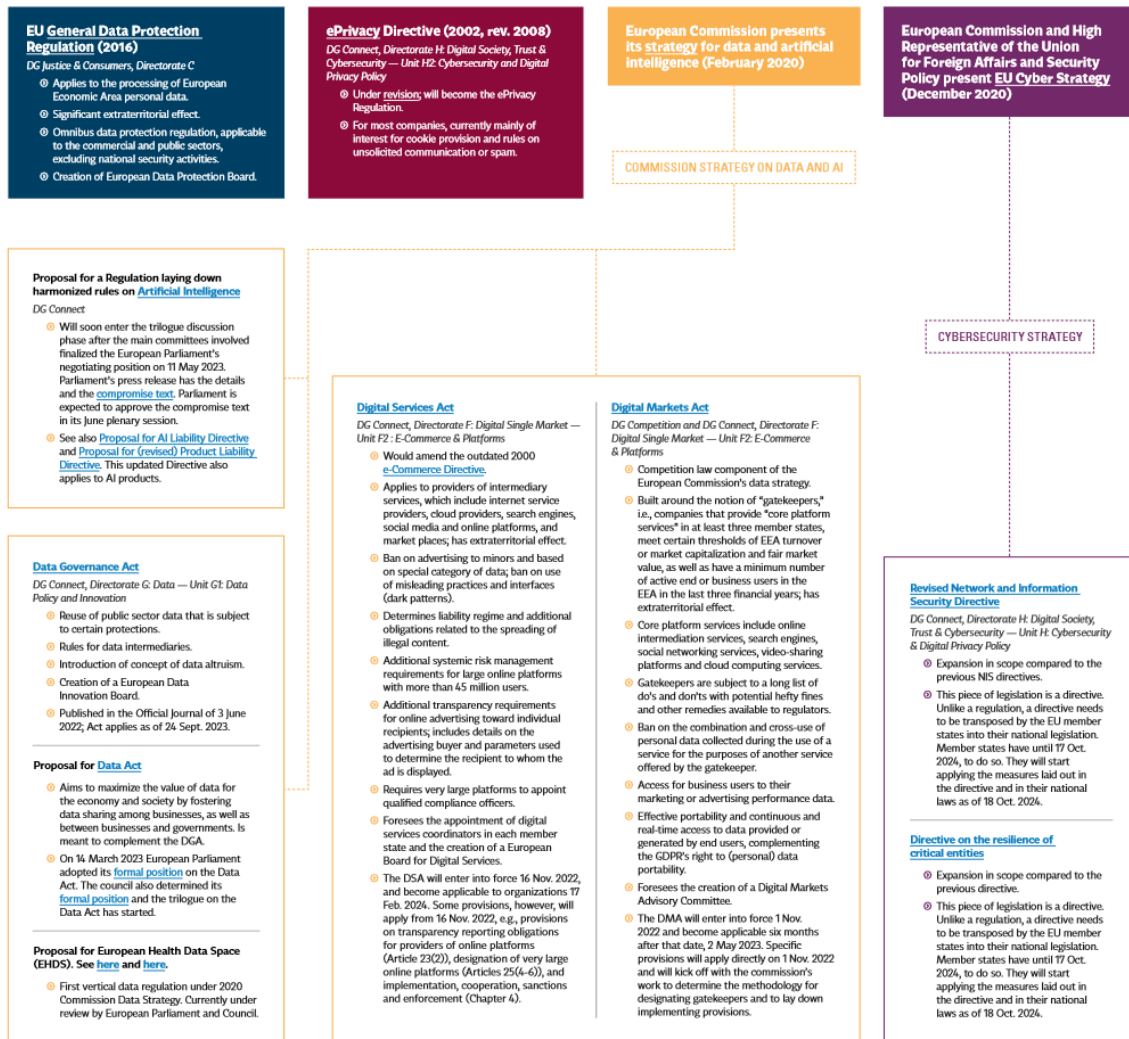
¹⁷⁷¹ *Verwaltungsgericht Wiesbaden*. Judgment of 20 November 2021, Az. 6 L 738/21.WI, (1 December 2021).

¹⁷⁷² Felz, D. [Daniel] and Swire, P. [Peter]. (15 December 2021). *New EU data blockage as German court would ban many cookie management providers*. <https://iapp.org/news/a/new-eu-data-blockage-as-german-court-would-ban-many-cookie-management-providers>.

¹⁷⁷³ Knoke, F. [Friederike] and Stoklas, J. [Jonathan]. *Internationales Forschungsprojekt zu elektronischen Beweisen in Strafverfahren*, ZD-Aktuell 2015, <https://beck-online.beck.de/Dokument?vpath=bibdata%5Czeits%5Czdaktuell%5C2015%5Ccont%5Czdaktuell.2015.04724.htm>.

¹⁷⁷⁴ Chapter II, Section 3.8.1.

¹⁷⁷⁵ Chapter II, Section 3.8.2.



Source: IAPP, "Global Privacy Law and DPA Directory"¹⁷⁷⁶

Based on the EU's Better Regulation approach¹⁷⁷⁷, Commission, Council and Parliament constantly review regulatory instruments of the EU. In a Pilot Project, requested by the European Parliament, managed by the Commission, and carried out by a contractor, it was found "that while much of the relevant law is compliant with the standards and requirements of the EU's data protection framework and relevant jurisprudence, there are also shortcomings and issues that require further attention from the legislator and supervisory authorities."¹⁷⁷⁸ The first task of this project was to "catalog legislation, instruments or agreements in the Area of Freedom, Security and Justice that involve the processing of personal data that authorizes or allows the processing of personal data in relation to law enforcement and law enforcement agencies on the basis of the EU Charter of Fundamental Rights and the European Convention on Human Rights"¹⁷⁷⁹ which resulted in 77 regulatory instruments being assigned to this catalog. This shows the fragmentation of the instruments and the challenge for the EU legislative to react to developments by drafting or revising regulations so that they meet the requirement of consistency. These challenges are particularly strong in those regulatory areas where it

¹⁷⁷⁶ IAPP. (May 2023). *Infographic: EU Data Initiatives in Context*. https://iapp.org/media/pdf/resource_center/recent_eu_data_initiatives_in_context_infographic.pdf.

¹⁷⁷⁷ See also Chapter I, Section II.4.

¹⁷⁷⁸ Fondazione Giacomo Brodolini. (1 December 2018). *Fundamental rights review of EU data collection instruments and programmes, final report*, https://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf. P. 1.

¹⁷⁷⁹ Fondazione Giacomo Brodolini. (1 December 2018). *Fundamental rights review of EU data collection instruments and programmes, final report*, https://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf. P. 1–2.

is necessary to bring diverse, usually conflicting interests into practical concordance. One such area is Freedom, Security and Justice, where the interests of law enforcement, the protection of suspects, the sovereignty of other States and the interests of participants in the digital economy overlap. As explained above¹⁷⁸⁰, the current situation may put ISPs and CSPs in a precarious position from the point of view of the rule of law, since access to personal data in the cloud is carried out by exploiting legal gray areas and by cooperating with ISPs in a way that privatizes legal assistance. Balancing these interests is a complex task for the legislature.

Most of the adaptive measures as a reaction to this fragmentation were planned between the end of 2020 and the end of 2021. This highlights the long-time span of five years between the adoption of an instrument (e.g., GDPR in 2016) and the adaptation of other instruments to the former (2021); this period cannot keep pace with the ever-faster development in a global ecosystem of transborder data flows. The Commission could therefore be exposed to the accusation from – for instance – the US side that the EU makes high regulatory demands on the agreements with third countries but has not yet implemented their own demands in the European framework in a harmonizing manner. An example for the challenge of consistency is the demarcation between the GDPR, the LED, the EIO Directive, the E-Privacy Directive, the DGA, and the DMA.

In its communication on a “way forward on aligning the former third pillar *acquis* with data protection rules”, the Commission set out the results of its review and specified ten legal acts that should be aligned with the LED and a timetable for doing so.¹⁷⁸¹ These measures for alignment can be assigned to different areas in which legislations require improvement.¹⁷⁸² The focus of these alignments lies on two points: First, on the inclusion of essential guarantees, which result from the GDPR, guidelines or recommendations of WP29, EDPB, or EDPS, and the case law of the CJEU. Second, the need to clarify that any processing of personal data under one of the instruments to be improved is subject to either the LED or the GDPR, depending on whether it takes place in the context of criminal or non-criminal proceedings. With regard to the relationship between the EU-US MLAT¹⁷⁸³ and the LED, the Commission found that the EU-US MLAT does not have to be amended because it contains – through the EU-US Umbrella Agreement¹⁷⁸⁴ – enough appropriate safeguards for the protection of personal data.¹⁷⁸⁵ The Commission did not issue a finding on a possible alignment with the PNR Directive¹⁷⁸⁶, because the “PNR Directive was subject of a preliminary reference lodged to the Court of Justice of European Union in which its compatibility with Articles 7, 8 and 52(1) of the Charter is

¹⁷⁸⁰ Chapter III, Section II.1.2.7.

¹⁷⁸¹ European Commission. *Communication from the Commission to the European Parliament and the Council, Way forward on aligning the former third pillar *acquis* with data protection rules*, COM(2020) 262 final, (25 June 2020).

¹⁷⁸² Purpose limitation (7 measures): 2002/465/JHA, 2005/671/JHA, 2008/615/JHA, 2008/616/JHA, 2009/917/JHA, L 39/20, 2014/41/EU. Reference to the LED (7): 2006/960/JHA, 2007/845/JHA, 2008/615/JHA, 2008/616/JHA, 2009/917/JHA, 2014/41/EU, 2015/413. Define data categories (5): 2005/671/JHA, 2006/960/JHA, 2007/845/JHA, 2008/615/JHA, 2008/616/JHA. Data subjects rights (3): 2008/615/JHA, 2008/616/JHA, L 39/20. Data retention and protocolization (3): 2008/615/JHA, 2008/616/JHA, L 39/20. Information obligation (3): 2008/615/JHA, 2008/616/JHA, 2015/413. Transfer to third countries / international organizations (2): 2008/615/JHA, 2008/616/JHA. Data security and data quality (2): 2009/917/JHA, L 39/20. Proportionality (1): 2006/960/JHA. References to the horizontal data protection framework (1): 2006/960/JHA. Coordinated Supervisory Agencies Model (1): 2009/917/JHA. Guarantees for processing special data categories (1): L 39/20.

¹⁷⁸³ EU. *Agreement on mutual legal assistance between the European Union and the United States of America*, OJ L 181, 34–40, (19 July 2003).

¹⁷⁸⁴ See Chapter II, Section II.4.4.

¹⁷⁸⁵ “In addition to the safeguards included in the Agreement, the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (‘EU-U.S. Umbrella Agreement’), in force since February 2017, complements the Agreement with appropriate safeguards for the protection of personal data, and therefore there is no need for further alignment of the EU-U.S. MLAT.” European Commission. *Communication from the Commission to the European Parliament and the Council, Way forward on aligning the former third pillar *acquis* with data protection rules*, COM(2020) 262 final, (25 June 2020). P. 5.

¹⁷⁸⁶ See Chapter II, Section II.3.6.

being examined. The Commission will assess the need for any data protection-related revision of the PNR directive in the light of the Court's ruling.¹⁷⁸⁷

Another initiative aims to align the data protection rules of the EIO Directive¹⁷⁸⁸ with those of the LED to create a solid and coherent data protection framework for the Union.¹⁷⁸⁹ For a processing of personal data carried out in accordance with the EIO Directive, depending on whether in the context of criminal or non-criminal proceedings, the provisions of LED or GDPR apply.

In the above-mentioned case of the *Verwaltungsgericht Wiesbaden*, it also became clear that it is difficult to draw a line between the E-Privacy Directive and the GDPR. The question arose whether the GDPR is applicable to the data processing at all. This is because the “data exchange” between Akamai Inc./GmbH¹⁷⁹⁰ and Cybot A/S¹⁷⁹¹ could be a telecommunications service, the permissibility of which could be governed by the respective national implementation law of a Member State due to the area exception for the E-Privacy Directive stipulated in Art. 95 GDPR.

Since the DGA includes rules for different types of intermediaries who process both personal and non-personal data, its interplay with the GDPR becomes important.¹⁷⁹² The DGA is without prejudice to all regulatory instruments described in Chapter II Section II.3 of this thesis, it shall not prevent TFPD in accordance with Chapter V of the GDPR from taking place.¹⁷⁹³ It is noticeable that some rules of the DGA are dealt with in the Recitals, but not so in the norm text itself. Those rules are central requirements for intermediaries, especially on contractual terms and conditions, definitions of “general interest”, and technical-organizational measures. Although the principle of purpose limitation is standardized, the DGA does not contain rules on how this is to be secured; greater consideration should therefore be given to the principles of data protection through Privacy by Design and Privacy by Default, as Roßnagel also noted.¹⁷⁹⁴ Moreover, Recital 6 of the DGA states that, “insofar as personal data are concerned, the processing of personal data should therefore rely upon one or more of the grounds for processing provided in Art. 6 GDPR.”¹⁷⁹⁵ However, it is not clear whether all requirements of the GDPR also apply in the context of processing scenarios under Chapter II of the DGA. It would have been helpful to clarify, for example, in the case of consents to process personal data for purposes in the general interest other than scientific research purposes, that a specified and legitimate purpose must be identified so that consent can be given freely, specific, and informed. The EDPB found also that “the DGA entails several significant inconsistencies with the GDPR, notwithstanding the statement in the Recital that it is “without prejudice” to the GDPR. The EDPB urged the co-legislators of the DGA to address the important criticalities, thus avoiding that the DGA creates a

¹⁷⁸⁷ European Commission. *Communication from the Commission to the European Parliament and the Council, Way forward on aligning the former third pillar acquis with data protection rules*, COM(2020) 262 final, (25 June 2020). P. 12.

¹⁷⁸⁸ See also Chapter II, Section II.3.7.

¹⁷⁸⁹ European Commission. *Proposal for a Directive of the European Parliament and of the Council amending Directive 2014/41/EU, as regards its alignment with EU rules on the protection of personal data*, 2021/0009 (COD), (20 January 2021).

¹⁷⁹⁰ The cookie service provider from Denmark uses the services of the company Akamai Technologies Inc. in the US for its services by using server capacities of Akamai

¹⁷⁹¹ The company of the cookie consent service “Cookiebot” offered from Denmark

¹⁷⁹² European Commission. *Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, COM(2020) 767 final, (25 November 2020). P. 1.

¹⁷⁹³ European Commission. *Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, COM(2020) 767 final, (25 November 2020). Recital 3.

¹⁷⁹⁴ Roßnagel, A. [Alexander]. (2021). Grundrechtsschutz in der Datenwirtschaft. *Zeitschrift für Rechtspolitik*, 54(6), 173–176. P. 175.

¹⁷⁹⁵ European Commission. *Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, COM(2020) 767 final, (25 November 2020). Recital 6.

parallel set of rules, not consistent with the GDPR, as well as with other Union law”.¹⁷⁹⁶ To address inconsistencies, EDPB urged to carefully consider the interplay between the DGA and the GDPR, the definitions/terminology use in the DGA, and to make sure that the fundamental requirements of GDPR like the appropriate legal base and derogations for special categories of personal data. The GDPR sets high requirements for data exchange and covers a wide scope, including pseudonymized data. Although the Commission argued that the DGA is logically and coherently linked to other initiatives announced in the Data Strategy,¹⁷⁹⁷ it did not significantly address this conflict of conflicting legal principles. This can lead to paradoxical results. A company that enables data access and spends a great deal of effort to meet all data protection legal requirements to do so would be obligated under the DGA to provide the data it collects. A company that, for strategic reasons, wants to put less effort into its compliance with the new Data Strategy instruments, on the other hand, could refuse data access with a reference to the GDPR. Data protection could then collide with the “data fungibility” within the DGA and become a competitive disadvantage. It is therefore at least questionable how the Commission would deal with interactions between data protection law and data economic law. It is to be hoped that the conflict between data access and data protection will be taken into account in the course of further political discussion. Additional exceptions would have to be created to leave the provision of data in certain cases to the discretion of such companies. Otherwise, such companies would run the risk of having to choose between compliance with data protection regulations on the one hand and data access regulations on the other.

The DGA should also supplement another measure, the Open Data Directive. Personal data fall outside the scope of the Open Data Directive insofar as this Directive excludes or restricts access to such data for reasons of data protection, privacy and the integrity of the individual, in particular in accordance with data protection rules.¹⁷⁹⁸

Overlapping enforcement workflows of the European framework also fit in with the discussion around inconsistencies. The IAPP noted

that an act or omission by a gatekeeper may constitute a violation of the DMA and, simultaneously, the GDPR. This could create issues because both statutes have different enforcement mechanisms, different regulators and different sanctions. While the DMA indicates its provisions are “without prejudice” to the GDPR, nothing indicates how these situations need to be addressed. The EDPS and EDPB have both expressed concern over potential conflicts and escalations in their respective opinion 2/2021 and statement on the DSA and Data Strategy package.¹⁷⁹⁹

This is one of the reasons why more and more voices have been raised to envisage “alternative models of enforcement of the GDPR, including a more centralized approach”¹⁸⁰⁰. This may be due to the fact that – most recently in the draft version of the E-Privacy Regulation – a paradigm shift has taken place in cross-border criminal justice by replacing the classic territoriality principle with the *lex loci solutionis*. This leads to an obligation of ISPs active in one EU Member State to provide foreign Member State data.

¹⁷⁹⁶ EDPB. *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf, (19 May 2021), P. 2.

¹⁷⁹⁷ European Commission. *Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, COM(2020) 767 final, (25 November 2020). P. 1.

¹⁷⁹⁸ European Commission. *Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, COM(2020) 767 final, (25 November 2020). Recital 7.

¹⁷⁹⁹ Tielemans, J. [Jetty]. (1 December 2021). *The EU's DMA and DSA: Why this should be of interest to privacy pros*. <https://iapp.org/news/a/developments-on-the-dma-and-dsa-why-this-should-be-of-interest-to-privacy-professionals>.

¹⁸⁰⁰ Manancourt, V. [Vincent]. (2 December 2021). *Top EU official warns privacy rules may need to change*. *Politico*. <https://www.politico.eu/article/eu-privacy-regulators-clash-gdpr-enforcement>.

This can lead to “enforcement bottlenecks” as described above¹⁸⁰¹. A debate has therefore arisen “on who should have the right to enforce the bloc’s [Union’s] privacy rules between member countries where Big Tech companies have established their headquarters – namely Ireland and Luxembourg – and major institutions like the European Commission, the European Data Protection Supervisor’s (EDPS) office, in charge of policing EU institutions, and the EDPB”¹⁸⁰².

The Commission should continue to study the challenges posed by emerging technologies and close gaps through regulations. The latter could also be area-specific, which on the one hand would more suitably include developments such as Big Data, “blockchain” applications, IoT, facial recognition and AI technology, but on the other hand could increase the complexity of the European framework by raising the number of points of contact between various regulatory instruments. The Commission partially included these challenges in two strategy papers: the “EU-US agenda for global change” and - in more detail - the “European Strategy for Data”.¹⁸⁰³ The Commission had therefore asserted that “the GDPR is an important component of the human-centric approach to technology and a compass for the use of technology in the twin green and the digital transitions that characterizes EU policy-making. This has been highlighted more recently by the White Paper on Artificial Intelligence and the European Strategy for Data of February 2020.”¹⁸⁰⁴ What is remarkable about the GDPR is that it does not (yet) contain protections that correspond to the specific risks of using data for AI systems and Big Data evaluations. The abstractness and generality of its rules provide room for litigation and the opportunity for powerful interests to prevail in the interpretation and application of these rules. Roßnagel therefore argued that they do not provide sufficient specific protection for the fundamental rights of data subjects.¹⁸⁰⁵

To meet its goals, the GDPR should be improved by eliminating these inherent deficits. The evaluation of the GDPR by the Commission – regulated in Art. 97 GDPR – offered a good opportunity for this. This evaluation took place for the first time in June 2020.¹⁸⁰⁶ According to Art. 97(2) GDPR, the Commission has “in particular” to review the application and functioning of Chapters V and VII of the GDPR. However, the Commission did not limit its evaluation to these Chapters. From the Commission’s point of view, the GDPR has proven its worth. It achieved its goals of strengthening the rights of the data subjects and ensuring the free movement of data in the Union.¹⁸⁰⁷ The Commission acknowledged that there are areas in which improvements could be made in the future but did not propose concrete changes. It assumed that most of the problems

¹⁸⁰¹ Chapter IX, Section I.1.4.

¹⁸⁰² Manancourt, V. [Vincent]. (2 December 2021). Top EU official warns privacy rules may need to change. *Politico*. <https://www.politico.eu/article/eu-privacy-regulators-clash-gdpr-enforcement>.

¹⁸⁰³ European Commission. *A new EU-US agenda for global change*, JOIN(2020) 22 final, (2 December 2020). // European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020).

¹⁸⁰⁴ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 1.

¹⁸⁰⁵ Roßnagel, A. [Alexander]. (2021). Grundrechtsschutz in der Datenwirtschaft. *Zeitschrift für Rechtspolitik*, 54(6), 173–176. P. 175.

¹⁸⁰⁶ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020).

¹⁸⁰⁷ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 4.

identified by Member States and stakeholders would likely be resolved with more experience with the application of the GDPR over the coming years.¹⁸⁰⁸

The Commission also analyzed the global reach of the GDPR. Many States outside the EEA have adopted data protection laws, for which the Commission was able to find, according to Art. 45 GDPR, that they offer an adequate level of protection. However, any process of such an adequacy decision is lengthy, which is why there are also opinions that “the European Union’s approach is the mistaken logic that this country-by-country assessment approach is effective in promoting better data privacy and protection by companies that manage personal data”¹⁸⁰⁹. Nevertheless, the need to review adequacy decisions and to ensure the continuity of such decisions “has prompted several of these countries and territories to modernize and strengthen their privacy laws”.¹⁸¹⁰ The adequacy decision on 17 December 2021 regarding the Republic of Korea is the most recent one at the time of closing the research for this thesis,¹⁸¹¹ and exploratory talks are ongoing with other important partners in Asia and Latin America.¹⁸¹² The GDPR has, according to the Commission,

emerged as a key reference point at international level and acted as a catalyst for many countries around the world to consider introducing modern privacy rules. [...] The adoption of the GDPR has spurred other countries in many regions of the world to consider following suit. This is a truly global trend running from Chile to South Korea, from Brazil to Japan, from Kenya to India, and from California to Indonesia. The EU’s leadership on data protection shows it can act as a global standard-setter for the regulation of the digital economy.¹⁸¹³

The Commission considered SDPC as the “by far the most widely used data transfer mechanism, with thousands of EU companies relying on them in order to provide a wide range of services to their clients, suppliers, partners and employees.”¹⁸¹⁴ This is also underscored by an IAPP-EY Privacy Governance Report, which found that SDPC are used by nearly all (94%) of the 473 surveys that were completed.¹⁸¹⁵

Nevertheless, the Commission encouraged the EDPB to further work on the transfer tools, “including by further streamlining the approval process for binding corporate rules, finalizing the guidance on codes of conduct and certification as tools for transfers, and clarifying the interplay between the rules on international data transfers (Chapter V) with

¹⁸⁰⁸ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 4.

¹⁸⁰⁹ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

¹⁸¹⁰ European Commission. *Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information*, OJ L 76, 1–58, (19 March 2019).

¹⁸¹¹ European Commission. *Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, OJ L 44, 1–90, 24 February 2022.

¹⁸¹² European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 10.

¹⁸¹³ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 3 and 12.

¹⁸¹⁴ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 11.

¹⁸¹⁵ LaLonde, B. [Brandon] and Thompson, M. [Mark] and Kanthasamy, S. [Saz]. (2021). *IAPP-EY Annual Privacy Governance Report 2021*. <https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2021>. P. 23.

the GDPR territorial scope of application (Article 3)".¹⁸¹⁶ To strengthen the extraterritorial reach of the GDPR, the Commission believes that the involvement of the "controller's or processor's representative in the EU has to be pursued more vigorously".¹⁸¹⁷ To further promote convergence and international cooperation in the area of data protection, the Commission "intensified its dialogue in a number of bilateral, regional and multilateral fora to foster a global culture of respect for privacy and develop elements of convergence between different privacy systems". The Commission also wants to promote "data sharing with trusted partners while fighting against abuses such as disproportionate access of (foreign) public authorities to personal data."¹⁸¹⁸ Such abuse can arise from a situation where companies active in the European market are called based on a request to produce data for law enforcement purposes without full respect of EU fundamental rights. The Commission wants to solve this by concluding "appropriate legal frameworks with its international partners to avoid conflicts of law and support effective forms of cooperation" and "strengthening cooperation on the ground between European and international regulators".¹⁸¹⁹

To strengthen cooperation with countries worldwide with data protection legislation in place, the Commission announced in 2017 that they envisage to exercise their authority regulated in Art. 50 GDPR and to accede to Convention 108+.¹⁸²⁰ As Convention 108+ is closely aligned with the GDPR, the future of the GDPR will also have an impact on that of Convention 108+. The Commission also wants to ensure that other countries accede to Convention 108+,¹⁸²¹ and intends to work with the UN Special Rapporteur on data protection.¹⁸²² Furthermore, the cooperation for the protection of personal data between the Union and APEC is to be expanded. At the time, the Commission was pursuing the objective of convergence between the transfer tools of BCR and the CBPR.¹⁸²³ In the area of strengthening cooperation on law enforcement according to Art. 50(b) GDPR, the Commission formulated the goal of deepening cooperation with SAs in third countries.¹⁸²⁴ Specifically, the Commission could particularly examine ways of establishing mutual (administrative) assistance agreements among data protection supervisory authorities for the purpose of law enforcement by concluding a framework agreement for this purpose.

¹⁸¹⁶ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 11–12.

¹⁸¹⁷ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 12.

¹⁸¹⁸ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 12.

¹⁸¹⁹ European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020). P. 13.

¹⁸²⁰ CoE. *Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe*, <https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb>, (7 September 2020).

¹⁸²¹ European Commission, *Proposal for a decision authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, COM(2018) 449 final, (5 June 2018). P. 2–3. // European Commission. *Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalized World*, COM(2017) 7 final, (10 January 2011). P. 11.

¹⁸²² EDPS. *Resolution on Cooperation with the UN Special Rapporteur on the Right to Privacy*, https://edps.europa.eu/sites/edp/files/publication/15-10-27_cooperation_un_special_rapporteur_en.pdf, (28 October 2015).

¹⁸²³ APEC. *What is the Cross-Border Privacy Rules System?*, <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System>, (15 April 2019).

¹⁸²⁴ European Commission, *Proposal for a decision authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, COM(2018) 449 final, (5 June 2018). P. 11 ff.

The EDPB Strategy 2021-2023¹⁸²⁵ determined four main “pillars” of strategic objectives, as well as a set of key actions to help achieve those objectives. Along with advancing harmonization and facilitating compliance (pillar 1), supporting effective enforcement and efficient cooperation (pillar 2) and fostering the fundamental rights approach to new technologies (pillar 3), the EDPB wants to focus on “the global dimension” (pillar 4). The EDPB “is determined to set and promote high EU and global standards for international data transfers to third countries in the private and the public sector, including in the law enforcement sector” and reinforce its “engagement with the international community to promote EU data protection as a global model and to ensure effective protection of personal data beyond EU borders”.¹⁸²⁶ It proposed three key actions to do so:

- Promote the use of transfer tools ensuring an essentially equivalent level of protection and increase awareness on their practical implementation,
- engage in dialogue with international organizations and institutional networks in order to provide leadership in data protection and promote high standards of protection worldwide, and
- facilitate the engagement between EDPB members and the supervisory authorities of third countries with a focus on cooperation in enforcement cases involving controllers/processors located outside the EEA.¹⁸²⁷

III. Exogenous variables

The present Section III will first identify “archetypes”, to which national, supranational, or international regulations belong to. These archetypes are analytically distinct but can have overlaps in which they interact with each other. The reason for this overlap is the intermingling of stakeholder interests and arenas discussed in Sections I and II of this Chapter IX, that lead to the emergence of an archetype. To strive for a compromise in an international order, it is necessary to determine which elements from these archetypes could be used in a future solution to achieve the greatest possible acceptance by the stakeholders described in Section I of this Chapter, whose interests are reflected in the arenas described in in Section II of this Chapter. In Chapters II–VII, each regulatory measure was described within its framework, its respective set of norms, dogmatics, and handling in legal practice. The focus of this Section III now lies on making those measures understandable from the perspective of other frameworks. This Section III shall therefore “mirror” regulatory measures against archetypes, showcase where the differences and commonalities of these measures in question lie, and what the reasons, meanings, and purposes for such differences and commonalities are. It is therefore essential to “translate” those measures into domestic categories, and at the same time to immerse in the world of foreign law to find generic terms unencumbered by national pre-understanding. Therefore, the present Section III will also encompass comparative law principles.

The following geographical areas are mainly considered: Europe, US, APEC, ASEAN, China, OECD, UN, and WTO. Although India and the Russian Federation show significant developments in data protection law and interesting approaches for this thesis in terms of their type,¹⁸²⁸ they are mentioned only cursorily in the following, if at all. The

¹⁸²⁵ EDPB. *EDPB Strategy 2021-2023*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_strategy2021-2023_en.pdf, (15 December 2020).

¹⁸²⁶ EDPB. *EDPB Strategy 2021-2023*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_strategy2021-2023_en.pdf, (15 December 2020). P. 5.

¹⁸²⁷ EDPB. *EDPB Strategy 2021-2023*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_strategy2021-2023_en.pdf, (15 December 2020). P. 5–6.

¹⁸²⁸ For India, see International Association for Privacy Professionals. (25 July 2022). *Minister says India's Data Protection Bill 'a few months' away*. <https://iapp.org/news/a/minister-says-indias-data-protection-bill-a-few-months-away>.

reason for this, with respect to India, is that this country is “mostly focused on the domestic market, with no expansion ambitions so far, although the country is a strong voice among developing countries in international debates on issues related to the digital economy”; the Russian Federation “has influence mainly at a regional level, as a leading economy and driver of digital development in the Eurasian Economic Union”, however, both India and the Russian Federation have only a relatively limited global influence.¹⁸²⁹

The following comparison leaves out mechanisms such as the Privacy Shield, which, while important as an example of a cross-regional agreement, is more relevant as an implementing mechanism, as opposed to a normative regulatory framework. Moreover, China represents a deviation influenced by pragmatism, because it is not synonymous with its framework and, unlike the EU and US frameworks, blurs the classification of its own (in China’s case, APAC’s) framework, while at the same time being particularly significant to its framework. The following analysis will also include how a particular framework deals with (core) problems. The background is that this logically builds on Chapter VIII, should explain problems of compatibility or interoperability among the frameworks, and consider the multi-stakeholder approach being also problem oriented.

Apart from the assignment of archetypes, a future regulatory solution would have to ensure certain data protection principles and essential guarantees, which the stakeholders could agree upon based on their interests and the respective archetype applying to them. Those principles and guarantees will be discussed in Sections III.2 and III.3 of this Chapter.

1. Framework archetypes

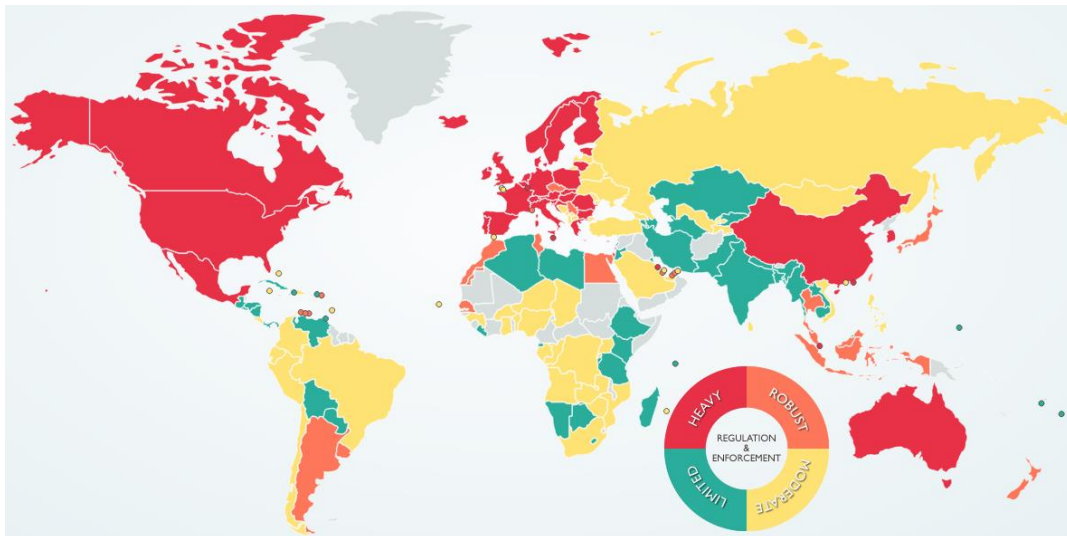
The preferred options of legislation taken by States “are deeply embedded in historical, legal and political traditions”¹⁸³⁰. The way in which countries approach their policies related to TFPD naturally reflects the underlying interests which have been analyzed in Section I of this Chapter. The aim of this Section III.1 is not to evaluate the appropriateness of any archetype; rather, it is to document the different approaches wherever they relate to TFPD.

Such approaches differ, sometimes widely. This makes classification difficult, time-consuming, and leads in practice to uncertainty for all stakeholders in a TFPD scenario. Common consulting practice in business often simplifies such a classification too much, based on categories such as, e.g., heavy / robust / moderate / limited.

// Although the Indian government has withdrawn this Data Protection Bill. See Singh, M. [Manish]. (4 August 2022). *India withdraws personal data bill that alarmed tech giants*. <https://techcrunch.com/2022/08/03/india-government-to-withdraw-personal-data-protection-bill>.

¹⁸²⁹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 108.

¹⁸³⁰ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 7.



Source: DLA Piper, "Compare data protection laws around the world"¹⁸³¹

However, at least the objective of this Section III.1 corresponds to that of this graphic. It is to make a classification of frameworks and to identify the principles and guarantees regulated as common or different. However, this thesis does not focus on a comparison of national rights to other national rights. The OECD did also not go so far as to assign each country to an archetype. The OECD justified this correctly by stating that a "country may apply several different approaches to cross-border data flows depending on the nature of the data involved. For instance, there can be differences across sectors [...] [and] some which refer to more sweeping categories of data, for instance, important data"¹⁸³².

The comparison shown graphically above is too imprecise for this thesis. Instead, the classification must be made not only from the point of view of a user in business and industry but based on clearly elaborated criteria. However, these criteria overlap and complicate the analysis. We decided to use the following five criteria:

- Objective
- Default position
- Legal force and jurisdictional reach
- Universal vs. limited approach to data governance
- Maturity

1.1. Objective

The reason for the approach in the US framework was already at the beginning of the 1980s "a fear that placing unnecessary or unwarranted controls and barriers over information technology will result in reducing its potential for economic and social benefits"¹⁸³³. The protection of personal data has traditionally been entrusted to the markets to support an open, interoperable, secure, and reliable internet that facilitates

¹⁸³¹ DLA Piper, (2023). *Compare data protection laws around the world*.

<https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=DE>.

¹⁸³² OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 18.

¹⁸³³ Pipe, R. [Russell]. (1984). International information policy: Evolution of transborder data flow issues. *Telematics*, 1(4), 409–418. P. 417–418.

the free flow of online information.¹⁸³⁴ The US framework assigns data to the function of a commodity. The economic value of data is particularly emphasized, so that any regulation initially represents a basically undesirable interference in the free market. Accordingly, when it comes to data protection, the market's self-regulatory powers are relied on and State regulation is only supported where necessary to create a functioning market, educate consumers or protect particularly vulnerable groups of individuals.¹⁸³⁵ Statutory provisions were only provided insofar as an individual's need for special protection against economic or public bodies was affirmed. The US has a leadership role in the global digital market. The technology sector with its data-driven products and in particular the VLOPs mentioned above¹⁸³⁶ have developed strongly, penetrated most markets of the world, and are further expanding into new markets. Therefore, the regulator in the US felt compelled to act, to adjust the free-market approach in some places and to intervene. On the one hand, the US "used trade agreements to ensure its firms unfettered access to foreign markets by, for example, favoring free data flows and banning practices such as data and server localization requirements"¹⁸³⁷. The reach of US-based data driven businesses made it increasingly difficult for US authorities to access their data stored overseas. The US Cloud Act was intended to counteract this. Third, "recent bans on activities of some foreign digital companies (e.g., Huawei, TikTok and Grindr) in the United States market also point towards more interventions of the State in the markets and increased restrictions related to data and cross-border data flows, for national security reasons"¹⁸³⁸. The US federal level does not grant a right to data protection like in the European framework's understanding. An explicit address of the right to privacy in US federal constitutional law does not exist. Rather, privacy is understood as the reasonable expectation of the individual to remain undisturbed by third Parties in a certain situation.

The US has an approach about the weight of data protection different to the European framework, which is exemplified by the emphasis on freedom of expression, economic interests, and public authorities' surveillance. Guarantees, however, are derived from individual constitutional provisions, in particular the fourth amendment of the US constitution.¹⁸³⁹ So far, the US Supreme Court left open whether there is a right to privacy as freedom unnamed in the US Constitution, except in limited contexts involving compelled disclosures surrounding abortion. The protection of privacy is therefore derived primarily from other freedoms, which leads to the fact that the US Supreme Court has defined it to have at least three distinct meanings. The first, a "right of personal privacy", is constitutionally protected to the extent the right can be deemed to involve decisions whose personal nature is "fundamental". The second determines privacy as something that an individual seeks to preserve as private, even in an area accessible to the public, provided that the individual has an actual, subjective expectation of privacy, and that expectation is "one that society was prepared to recognize as reasonable (so-called "reasonable expectation of privacy"). The protection of the fourth amendment is

¹⁸³⁴ Reidenberg, J. [Joel]. (2001). E-Commerce and trans-atlantic privacy. *Houston Law Review*, 2001, 717–749. P. 730–731. // Cunningham, M. [McKay]. (2013). Diminishing Sovereignty: How European Privacy Law Became International Norm. *Santa Clara Journal of International Law*, 11(2), 421–453. P. 441-442. // UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 100.

¹⁸³⁵ Kobrin, S. [Stephen]. (2004). Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 30(1), 111–131. P. 116.

¹⁸³⁶ Chapter II, Section II.3.8.2.

¹⁸³⁷ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 100.

¹⁸³⁸ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 102.

¹⁸³⁹ "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." USA. *Fourth amendment of the US constitution*, US congress, <https://www.archives.gov/founding-docs/bill-of-rights-transcript#toc-amendment-iv>, (15 December 1791).

more spatially oriented and requires physical interventions, even if more recent judgments of the US Supreme Court suggest an adjusted approach.¹⁸⁴⁰ The limits of this determination are obvious: Whenever personal data are not disclosed, then it is private; if it has been disclosed, it is not. According to the US Supreme Court, telecommunications connection data, for example, are therefore not protected because they are disclosed to the provider (so-called “third party doctrine”).¹⁸⁴¹ This changed when the US Supreme Court found that even when personal data has been disclosed to and is held by third Parties, this does not eliminate the existence of a lawfully protected privacy interest, because this information may nevertheless remain sensitive and subject to privacy protections. US State law does not deviate from the self-regulatory and market-oriented approach; rather, a measure is required only if it is necessary to establish a market. It enables then the Parties to meet on an equal footing and the consumer to compare conditions of individual offers. The US framework thus represents a “weak and patchy protection, partly due to the constitutional emphasis placed on freedom of expression and partly due to an entrenched cultural preference for market-based solutions”.¹⁸⁴² There are a “*salmagundi* of laws”¹⁸⁴³ at federal and State level that regulate sector specific data protection. Nevertheless, the “moves towards privacy regulation in some states in the United States, plus the proposed federal privacy regulation, may point to the tide turning towards a departure from the free market approach with giant digital companies”¹⁸⁴⁴.

The UN Guidelines were “rooted primarily in human rights concerns; commercial anxieties about restrictions on transborder data flows apparently took a back seat”.¹⁸⁴⁵ Justice Micheal Kirby, who headed the expert group responsible for drafting the OECD Guidelines 1980, the work of the OECD in this field was motivated primarily by economic concerns:

It was the fear that local regulation, ostensibly for privacy protection, would, in truth, be enacted for purposes of economic protectionism, that led to die initiative of the OECD to establish the expert group which developed its Privacy Guidelines. The specter was presented that the economically beneficial flow of data across national boundaries might be impeded unnecessarily and regulated inefficiently producing a cacophony of laws which did little to advance human rights but much to interfere in the free flow of information and ideas.¹⁸⁴⁶

In the APAC framework, agreements between APEC countries on data protection support the opportunity to liberalize and facilitate digital trade and commerce in Asia and the increase in transborder data flows. The CBPR facilitates legal compliance, it can help comply with data export restrictions, to promote consumer trust and ultimately access to and compliance with significant trading blocks in Asia. Within ASEAN, the objective is to “strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants, with a view to contribute to the promotion and growth of regional and

¹⁸⁴⁰ United States of America. *Carpenter v. United States*, Supreme Court, No. 16–402, (22 June 2018). Holding that an individual maintains a legitimate expectation of privacy in a detailed chronicle of his physical movements captured by technological means.

¹⁸⁴¹ See also Chapter III, Section I.

¹⁸⁴² Witzleb, N. [Normann] and Lindsay, D. [David] and Paterson, M. [Moir] and Rodrick, S. [Sharon]. (2014). An overview of emerging challenges in privacy law. In N. [Normann] Witzleb and D. [David] Lindsay and M. [Moir] Paterson and S. [Sharon] Rodrick, *Emerging Challenges in Privacy Law* (pp. 1–28). Cambridge University Press. P. 4.

¹⁸⁴³ Cunningham, M. [McKay]. (2013). Diminishing Sovereignty: How European Privacy Law Became International Norm. *Santa Clara Journal of International Law*, 11(2), 421–453. P. 441.

¹⁸⁴⁴ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 100.

¹⁸⁴⁵ Bygrave, L. A. [Lee A.]. (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar. P. 29.

¹⁸⁴⁶ Bygrave, L. A. [Lee A.]. (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar. P. 27.

global trade and the flow of information”¹⁸⁴⁷. ASEAN does not address restrictions on data flows. The APEC Privacy Framework 2015 “aims at promoting electronic commerce throughout the Asia Pacific region [...] and reaffirms the value of privacy to individuals and to the information society”, para. 5. Neither ASEAN nor APEC use the terms “fundamental right” and “human right” to define the protection of personal data.

As indicated above, China deviates from the APAC framework and is in this respect an archetype in its own. As UNCTAD stated,

contrary to the free-market approach of the United States, the Chinese economic and political system implies strong State intervention in the economy and society, which naturally translates into an approach towards State intervention in the digital economy, and therefore strict regulation of cross-border data flows. In China, policymakers control data and information, not only across borders, but also within the country, so as to maintain social stability and nurture knowledge-based sectors.¹⁸⁴⁸

This is because the domestic digital sector in China is growing even faster than in the US.¹⁸⁴⁹ This has led to economic tensions and measures affecting transfer mechanisms on both sides of this conflict.¹⁸⁵⁰ Other reasons are “weak domestic enforcement of intellectual property laws, adequate technological capabilities and resources, strong regulatory capacity, and strategic governmental and private investments in the digital sector”¹⁸⁵¹. Interestingly, China does not clearly distinguish between data protection and law enforcement purposes in its regulatory measures – as the European framework does – but has a minced double focus. As recently in the US, a tendency of a change can be observed in China, which results in China’s case in a “subtle shift in the country’s previously non-negotiable stance on cross-border data flows in recent months”¹⁸⁵². The reason for this change could be that “even though the predominant rationale for cross-border data regulation in China is national security and social stability, the economic agenda has become more central and critical to its data regulation policies over time”¹⁸⁵³; one important point within that agenda is to facilitate the digital component of the so-called “Belt and Road Initiative” (BRI)¹⁸⁵⁴. Although China is, as explained above¹⁸⁵⁵, improving its data protection framework, “the protection of privacy has not been a major priority, and China is a major player in terms of mass digital surveillance”. The Chinese approach for TFPD is ultimately still based on the central role of cybersecurity considerations in national security policy.¹⁸⁵⁶ However, in addition to the objectives of security and digital development, the human rights objective has also been added since the enactment of PIPL. The purpose of PIPL is to protect the rights and interests in

¹⁸⁴⁷ ASEAN. *Framework on personal data protection*, <https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf>, (November 2016). Para. 1.

¹⁸⁴⁸ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 102.

¹⁸⁴⁹ See above, Chapter I, Section I.2.

¹⁸⁵⁰ See below, Chapter IX, Section III.1.4.1.

¹⁸⁵¹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 102.

¹⁸⁵² UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 103.

¹⁸⁵³ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 102.

¹⁸⁵⁴ “China’s Belt and Road Initiative (BRI) development strategy aims to build connectivity and co-operation across six main economic corridors encompassing China and: Mongolia and Russia; Eurasian countries; Central and West Asia; Pakistan; other countries of the Indian sub-continent; and Indochina.” OECD. (2018). *China’s Belt and Road Initiative in the Global Trade, Investment and Finance Landscape*. <https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf>. P. 3

¹⁸⁵⁵ Chapter IV, Section IV.

¹⁸⁵⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 102. // See also Chapter VIII, Section I.2.

personal data and to promote the meaningful use of personal information. PIPL “is drafted on the basis of the Constitution” (Art. 1 PIPL) and included the right for the data subject to seek redress in courts if a company responsible for the processing of personal data refuses to comply with the request of a data subject to exercise its rights, Art. 50 PIPL. Overall, China outlines its objectives more flexible and from a more holistic perspective, including economic growth and social stability as key factors.¹⁸⁵⁷

The regulatory measures of the European framework are supposed to protect personal data and guarantee the self-determination of the individual, this framework thus emphasizes the control of data by individuals and is contrary to the approach of the US and China. As UNCTAD also noted, the Union “takes a strong regulatory approach towards the data-driven digital economy, which is based on the protection of fundamental rights and values of the European Union. In this sense, it is regarded as a human-centric approach”¹⁸⁵⁸. The Union aims to build a single digital market within its borders, wherein data are free to flow under a set of rules to protect private and public sector stakeholders.¹⁸⁵⁹ Digital integration into the regional market has been one of the focus areas of European policymakers in recent years. Regulation therefore “has taken place mostly in a defensive or reactive manner, as it aims to address the concerns stemming from the activities of global digital platforms”¹⁸⁶⁰. The EU is aware that it has only a relatively marginal share in the digital economy in relation to the US and China,¹⁸⁶¹ where most global digital platforms are based, and is trying to compensate for this through various policy initiatives. There is therefore a trend in the Union, especially through the Data Strategy¹⁸⁶², to distinguish more precisely between personal data that needs to be protected and such data that can be used for the purpose of developing innovations in particular, and the development of a digital single market in general. The GDPR postulates in Art. 1(2) that it protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. This has confirmed and again expanded the human-centric objective, so that those responsible for the processing of personal data theoretically must take all fundamental rights and freedoms into account, in all obligations and proportionality tests of the GDPR. Convention 108+ is primarily aimed “to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy” (Art. 1).

The objectives, and thus the general orientation of these frameworks, can therefore be summarized as follows:

Europe	Fundamental rights oriented
US	Trade oriented
APEC	Trade oriented
ASEAN	Trade oriented
China	Mixture between security-, trade-, and fundamental rights oriented
OECD	Trade oriented
UN	Fundamental rights oriented
WTO	Trade oriented

¹⁸⁵⁷ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 7.

¹⁸⁵⁸ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 104.

¹⁸⁵⁹ See Chapter II, Section II.3.8.1.

¹⁸⁶⁰ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 104.

¹⁸⁶¹ See Chapter I, Section I.2.

¹⁸⁶² See Chapter II, Section II.3.8.2.

1.2. Default position

Two types of default positions are relevant. The first concerns the lawfulness of the data processing activity as such and plays a role – as the “first stage test” under Directive 95/46 and the GDPR¹⁸⁶³ – for complying with the applicable requirements for lawful processing of personal data. The second – as the “second stage test” under Directive 95/46 and the GDPR¹⁸⁶⁴ – determines how frameworks differ in their approach to the lawfulness of TFPD of such data.

As to the first type of default position, GDPR and LED consider processing of personal data as a potential risk, forbid their processing as a principle (“prohibition principle”) and only allow such processing based on a certain legal ground. The ASEAN Framework on Personal Data Protection contains a prohibition with a reservation of permission in its para. 6(a). The APEC Privacy Framework 2015 has the weakest position within APAC, as it does not prohibit data processing but only encourages to prevent the misuse of personal data by meeting some obligations, paras. 14, 18. PIPL stipulates in Art. 13 that only under one of seven conditions may a data controller process personal data. PIPL provides, similar to the GDPR, multiple lawful basis for processing in addition to consent. In the US, the proposed ADPPA provides that a processing of covered data is generally permitted if it is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the individual to whom the data pertains (Sec. 101(a)(1) ADPPA); or a purpose expressly permitted by ADPPA (Sec. 101(a)(2) ADPPA). Sec. 101(b) ADPPA provides a list of such permissible purposes similar to those provided by Art. 6(1)(b)-(e) GDPR. However, ADPPA deviates from Art. 6(1)(f) GDPR because it does not provide for a generic term of “legitimate interest” with some degree of flexibility (and related balancing of interests) but defines interests of the covered entity that are considered legitimate. In the case of a transfer of covered data to a third party that relies on Sec. 101(a)(1) or (2) ADPPA, individuals have a right to opt out of such a transfer, Sec. 204(b) ADPPA. ADPPA includes in Sec. 102 and Sec. 204 a prohibition principle for certain types of sensitive personal data, which are

responding to a warrant or meeting heightened conditions for obtaining express affirmative consent of the individual when collecting, processing, or transferring biometric information, genetic information, aggregated internet browsing and search history, physical activity information, and transferring precise geolocation information to third Parties. Social Security numbers, password information, and nonconsensual intimate images are subject to further restrictions.¹⁸⁶⁵

Frameworks differ also in the second type of default position. Weber explained this type by stating that

on the one hand, the law could be based on an assumption that a transborder flow of data outside the jurisdiction should not take place unless a particular norm is in place allowing the transfer. On the other hand, the law does also have the possibility to presume that data flows are generally allowed unless the regulator exercises its authority to limit or forbid them in certain circumstances. Neither of the two default

¹⁸⁶³ See Chapter II, Section II.3.1.; and Chapter II, Section II.3.4.4.a.

¹⁸⁶⁴ See Chapter II, Section II.3.1.; and Chapter II, Section II.3.4.4.a.

¹⁸⁶⁵ USA, Senate Committee on Commerce, Science, and Transportation. *American Data Privacy and Protection Act Draft Legislation. Section by Section Summary*, <https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50>, (2022). P. 2.

positions is inherently better than the other, each of them has some advantages and disadvantages.¹⁸⁶⁶

The second type of default position distinguishes mainly between the GDPR (prohibition principle), China (restrictive), and the rest of the regulations (generally allowed, sometimes with limitations):

Europe	Aims at free data flow within the Member States and third countries with adequate level of protection. Some recent initiatives point to restrictions. The GDPR does not allow a transborder flow of personal data to third countries or international organizations unless a set of conditions is met to ensure compliance with the data protection rights provided to its Member States citizens. Onward transfers are subject to the same conditions.
US	ADPPA would not provide for additional requirements for transborder data transfers. ADPPA would include the prohibition principle for certain types of sensitive personal data.
APEC	Governments should ensure that there are no unreasonable impediments to TFPD while ensuring data protection and data security. Restrictions should be proportionate to risks. Onward transfers not mentioned (Principle of accountability applies).
ASEAN	Before transferring personal data to another country or territory, the organization should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organization will protect the personal data consistently with these principles.
China	Although China does not restrict all transborder data flows per se, it introduced various restrictions on specific data types and sectors. For instance, it requires OCII to store "important data," and "ordinary data" within China.
OECD	Transborder flows of personal data should not be restricted unless the recipient country does not substantially observe the Guidelines, or where no sufficient safeguards exist, or where the re-export of such data would circumvent domestic data protection legislation. A Member State may impose restrictions in respect of certain categories of personal data for which its domestic data protection legislation includes specific regulations in view of the nature of those data and for which the other Member State provides no equivalent protection. Member States should therefore take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member State, are uninterrupted and secure. Restrictions should be proportionate to the risks presented, considering the sensitivity of the data, and the purpose and context of the processing.
UN	When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.
WTO	No default position mentioned.

1.3. Legal force and jurisdictional reach

The international organizations framework and the APAC framework do not seek to displace or change an Economy's domestic laws but call on Member States to voluntarily implement their provisions. The regulatory measures of the two aim to endeavor, cooperate, promote and implement principles in their domestic regulations, and facilitate

¹⁸⁶⁶ Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130. P. 123.

the free flow of data among participating economies. Both provide minimum standards which can be supplemented by supplementary measures for data protection (the OECD Guidelines are capable of being supplemented by both national and international level). As soon as a company has acquired its membership, the data protection standards of the CBPR are binding. The directives of the EU and the Convention 108+ are also territorial and subject to national law. Convention 108 was the first legally binding international instrument in the field of data protection. Although Convention 108+ does also not explicitly supersede national rules, this regulatory measure is more forceful – stating that each “each Party shall take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application”, Art. 4(1) Convention 108. In contrast, regulations of the EU, such as the GDPR, are directly applicable on legislation in the EU Member States. Chinese laws and US laws are domestic rules by nature and therefore binding.

The reason for extraterritorial regulations in the US is also shaped economically, it aims at the establishment of an informational balance between the market participants and the protection of particularly vulnerable consumers. Extraterritorial regulations are used insofar as the registration of foreign participants in the domestic market is necessary to achieve these goals. In accordance with the economic focus, CPRA, ColoPA, VCDPA and the proposed Washington Privacy Act apply to businesses which meet one or more of some thresholds¹⁸⁶⁷ even if they do not have a physical presence in their respective State. At US federal level, the US Cloud Act has an extraterritorial reach. As defined in ADPPA, a covered entity is “any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.)”, plus nonprofits and common carriers. “Transfer means to disclose, release, share, disseminate, make available, or license in writing, electronically, or by any other means”, not necessarily a transborder transfer. The Federal Trade Commission Act provides the FTC with authority to police unfair or deceptive acts or practices “in or affecting commerce” in the US. This might also include “acts or practices involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States; or involve material conduct occurring within the United States”, 15 U.S.C. Section 45(a)(4)(A). ADPPA would therefore have a potential extraterritorial effect and could lead to litigation in the US for companies engaged in international trade.

The provisions of Directive 95/46 were limited to the regulation of data processing taking place in the Union. The applicability of Directive 95/46 reached its limits if a controller had no headquarter or data processing center within the EU – or at least an establishment in the context of whose activities the processing is carried out. This created gaps in protection. The applicability of European law to non-European services was not clear and associated with problems, which the exploitation of this weakness through “forum shopping” by VLOPs showed. Under the GDPR, those responsible for data processing can no longer evade the provisions of the GDPR by pointing out that the processing of personal data takes place outside the EU/EEA. Extraterritorial sovereignty is claimed in the GDPR in Art. 3(1) GDPR by the criterion of “a processing in the context of the activities of an establishment of a controller or processor in the EU”; and Art. 3(2) GDPR extends the application of EU law to the processing of personal data by a controller not established in the EU in some instances, regardless of whether the processing is carried out in the context of the activities of an establishment of a controller or a processor in the Union. This widened the extraterritorial reach of the GDPR compared to Directive 95/46.

¹⁸⁶⁷ See Chapter III, Section II.2.

China recognizes the extraterritorial effect of data protection law. Under the DSL, any organization or individual outside the territory of mainland China may also be held accountable to the law if such organization or individual harms the national security, public interests, or the lawful rights and interests of citizens or organizations of mainland China in carrying out data processing activities. The DSL therefore has extraterritorial reach. PIPL determines its jurisdiction in Arts. 3(1) and 3(2) PIPL. Art. 3(1) PIPL does so if foreign organizations process or handle the personal information within the territory of China. This provision is similar to Art. 3(1) GDPR; nevertheless, PIPL highlights expressly the necessity of establishing a special agency or designating a representative within the borders of the PRC to be responsible for matters related to the personal data an organization handles, Art. 53 PIPL. Moreover, PIPL applies its jurisdiction in Art. 3(2) to the activities carried out outside the territory of the PRC to process the personal data of natural persons within the territory of the PRC under some certain conditions. These are where the processing is for the purpose of providing products or services to natural persons within the Mainland China; where the processing includes analysis and evaluation of the behaviors of natural persons within the Mainland China; and where other circumstances prescribed by laws and administrative regulations occur. The meaning of “analysis and evaluation” here is very broad and seems to cover “monitoring” activities as in Art. 3(2) GDPR. Nevertheless, Art. 3(2) GDPR and Art. 3(2) PIPL have differences. The GDPR is based on the “targeting criterion”, whereby it must be assessed whether the conduct of those responsible for the processing abroad shows their apparent intention to offer goods or services to data subjects in the EU; inadvertent or incidental provision of services is not enough.¹⁸⁶⁸ PIPL focuses not only on the criterion whether this processing has purpose, but also on whether those responsible have processed personal data of a natural person in China, which corresponds more to an “effects criterion” instead of a sole “targeting criterion”. The Art. 3(3) GDPR condition is not included in the PIPL, which instead shall apply to “other circumstances as stipulated by laws and administrative regulations”.

Legal force and jurisdictional reach can therefore be summarized as follows:

	Legal force	Jurisdictional reach
Europe	Binding	Extraterritorial
US	Binding	Extraterritorial (State level laws: California, Colorado, Virginia; Federal level law: Cloud Act)
APEC	CBPR: Binding on participating organizations	Not extraterritorial
ASEAN	Nonbinding	Not extraterritorial
China	Binding	Extraterritorial
OECD	Nonbinding	Not extraterritorial
UN	Nonbinding	Not extraterritorial
WTO	Nonbinding	Not extraterritorial

1.4. Universal vs. limited approach to data governance

The stakeholders with their interests, identified in Section I of this Chapter IX, engaged in activities to form norms within the global ecosystem of transborder data flows. However, there is no single forum for all issues related to global data governance; rather, their activities overlap or even counteract each other. The UN noted that “when it comes

¹⁸⁶⁸ EDPB. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation.* (12 November 2019). P. 12 ff.

to the governance of cross-border data flows, there is no one-size-fits-all approach”¹⁸⁶⁹. Nevertheless, the approaches can be assigned, as the WEF did, to a so-called “architecture for global data governance”.¹⁸⁷⁰ Therein, for each different and non-mutually exclusive “element” of such governance, the forming of norms can be divided into “universal availability” and “limited participation”.

Elements	Universal availability	Limited participation
Transfer mechanisms	Unilateral openness	Adequacy recognition
	Legitimate grounds	Certification programs
	Accountability-based	Trusted entity schemes
Regulatory cooperation	Binding international agreements on legal harmonization	Regional model laws
		Principles and guidelines
		MLATs
Technical standards	Standard-setting in multistakeholder forums	National and regional standard-setting
		Exclusive data spaces initiatives and consortium
		Bilateral mutual recognition agreements or equivalence decisions
International trade rules	WTO GATS	Digital trade commitments
	WTO JSI	

1.4.1. Transfer mechanisms

This Section III.1.4.1 will focus on the element of how the different frameworks treat a TFPD from a governance perspective, which the OECD has described as an “indicative taxonomy, albeit with blurred boundaries between the different categories”.¹⁸⁷¹ Within a “transfer mechanism” of a framework, a distinction is made as to whether, first, the transfer instruments are general in scope or sector specific, second, what level of restrictiveness to the flow of personal data these instruments have, and, third, how data flow restriction types can be classified.

It is possible that some frameworks have not yet implemented a regulatory framework for data protection and, as such, have not imposed any regulations that affect TFPD, which means that such data therefore flow freely across borders by default. Such frameworks are then not analyzed in the further considerations.

As TFPD are common to most sectors, transfer mechanisms usually have a “general” scope of application across all sectors. The GPDR is the most significant example of this category. Other countries that have already been recognized by an adequacy decision of the Commission, or that have an essentially equivalent level of protection as interpreted by the CJEU, also fall under this category; with the exception of Canada, which has been recognized as having an adequate level of protection only for its commercial organizations.

¹⁸⁶⁹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 100.

¹⁸⁷⁰ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 14.

¹⁸⁷¹ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 17.

Australia, the United Arab Emirates and the United Kingdom reduce the scope to the health sector, the Republic of Korea to web mapping data.¹⁸⁷² The US requires defense-related data to be stored in domestic cloud servers;¹⁸⁷³ moreover, an EO by POTUS gives the US Department of Justice enlarged powers to stop foreign adversaries like those from China accessing Americans' personal data, while at this stage only health data are explicitly mentioned as being in scope.¹⁸⁷⁴ Several countries require local data storage in sectors, such as financial data, insurance data, electronic payments, telecommunications data and gambling data.¹⁸⁷⁵ It should also be noted here again that a framework cannot always and in its entirety be classified as solely belonging to one category or another. The European framework shows in the Union's Data Strategy also elements of a sector specific regulation, especially in the development of strategically important areas such as manufacturing, agriculture, health, and mobility that go hand in hand with the development of sector specific data spaces.

China imposes different requirements for "core data", "important data," and "ordinary data" in Art. 21 DSL, Art. 37 CSL and Art. 40 PIPL limit a TFPD whenever an OCII wishes to make such a transfer, or whenever a non-OCII wants to transfer "important data" or large amounts of personal data. China therefore focuses its scope on specific data types and specific sectors of the data economy.

The level of restrictiveness can also be divided into certain categories. One category allows a TFPD but foresees an ex-post accountability of the respective data exporter, another makes such transfer subject to various types of safeguards, and a third encompasses the "strictest" mechanism subject to ad-hoc authorization. UNCTAD divided these categories similarly. Its "light touch approach" corresponds to the first category, its "prescriptive regulatory approach" to the second category. UNCTAD further divided the third category into "restrictive" and "guarded" mechanisms which "tend to focus primarily on localization regulations, although their predominant policy rationales are quite different"¹⁸⁷⁶. The differences between these categories can be marginal and fluid, the "difference between guarded, restrictive and prescriptive approaches is not always clear in practice"¹⁸⁷⁷ and "countries may shift across these groups"¹⁸⁷⁸ depending on their regulatory resources. UNCTAD further noted that

with increased regulatory capacity, emerging economies may choose to impose stronger prescriptive requirements, instead of localization measures, for personal data protection. Further, some highly prescriptive compliance requirements for cross-border data flows may effectively amount to a restrictive approach when cross-border data flows are largely impermissible. Similarly, certain countries that adopt a guarded approach to maximize economic gains could also be hoping to achieve political control

¹⁸⁷² UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 124.

¹⁸⁷³ USA, Department of Defense. *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)*, <https://www.federalregister.gov/documents/2016/10/21/2016-25315/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for>, (16 October 2016).

¹⁸⁷⁴ USA, The White House. *Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States*, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states>, (15 September 2022).

¹⁸⁷⁵ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 124–125.

¹⁸⁷⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 136.

¹⁸⁷⁷ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 136.

¹⁸⁷⁸ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 138.

over domestic data and vice versa. Finally, countries adopting a light-touch approach may impose localization requirements in sensitive sectors.¹⁸⁷⁹

One example of such “highly prescriptive” mechanism is, often raised as a major criticism against the GDPR, a “*de facto* restriction” on TFPD imposed by the extraterritorial reach of the GDPR.¹⁸⁸⁰

Mechanisms that allow a free TFPD provide for ex-post accountability for the data exporter. This means that the data exporter remains accountable, sometimes also by the fact that an individual (“local representative”) who can be held accountable has to be assigned, for ensuring that all processing of personal data conducted abroad is consistent with domestic laws. This principle of accountability applies to Mexico, Canada, Australia, Singapore and the Philippines.¹⁸⁸¹ None of the sector specific laws in the US contains a restriction on transborder data flows, although they impose relatively strong compliance requirements for all service providers.¹⁸⁸² The majority of companies in the US “must disclose certain data-privacy practices and adhere to those requirements, even when processing data outside the country, as they remain responsible for the data regardless of where it is processed. US companies mitigate these risks by stipulating requirements in relevant data-handling and processing contracts they implement with other companies.”¹⁸⁸³ Although both the CCPA and the CPRA do not explicitly regulate restrictions on TFPD, they can overlap and possibly conflict with certain restrictions in other frameworks, which in practice can then lead to addendums to contractual requirements under domestic law as a starting point to reach compliance with other frameworks’ requirements.

For instance, the CCPA requires companies that hold personal data to meet some of the same contractual obligations as required under the GDPR and PIPL, including contractual addendums between a “business” and its “service providers” (as those terms are defined under the CCPA) that: Specify the limited purpose for the sharing or disclosure of personal information. Obligate the third-party recipients to the same level of privacy protection as the CCPA.¹⁸⁸⁴

A transfer according to ADPPA is the disclosure of data by transmission regardless of whether or not the recipient is located in the US. Unlike the GDPR in Chapter V, ADPPA does not provide for additional requirements for international data transfers. Therefore, the same conditions apply as for a domestic transfer, with only one deviation: ADPPA would require as content of a covered legal entities’ privacy policy to disclose if covered data shall be transferred to the PRC, Russia, Iran, or North Korea.

Kuner divided transfer mechanisms into “geographically-based” and “organizationally-based”.¹⁸⁸⁵ The geographically-based mechanism is used by countries to “protect against risks posed by the country or location to which the data are to be transferred, while the organizationally-based approach targets risks posed by the organizations which receive

¹⁸⁷⁹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 136.

¹⁸⁸⁰ See Chapter VIII, Section III.

¹⁸⁸¹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 128, 135, 137.

¹⁸⁸² UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 101.

¹⁸⁸³ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

¹⁸⁸⁴ Cooley LLP. (12 April 2022). *Cross-Border Data Transfers: PIPL vs. GDPR vs. CCPA*.

<https://www.jdsupra.com/legalnews/cross-border-data-transfers-pipl-vs-9241114>.

¹⁸⁸⁵ Kuner, C. [Christopher]. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD iLibrary, No. 187*. <https://doi.org/10.1787/5kg0s2fk315f-en>.

the data”¹⁸⁸⁶ In this respect, Kuner’s organizationally-based mechanism is synonymous with the ex-post accountability mentioned above. The geographically-based mechanism includes – according to Kuner – tests for the permissibility of data transfers that are contained in national legislation, such as whether the legal regime in the recipient country is adequate, comparable, or (essentially) equivalent (in general referred to as “adequacy”).

Again, there may be some overlap in categories. For example, the European framework includes the accountability principle, but also recognizes the adequacy mechanism. In addition to relying upon a positive adequacy decision, a data exporter can conduct TFPD by using accountability-based safeguards such as BCRs, SDPC, or other approved certification mechanisms.

A flow conditional on safeguards means that personal data can be transferred abroad subject to the data exporter and/or the recipient country complying with specified regulatory requirements. This category falls in the middle of the spectrum of mechanisms and is largely determined by requirements that refer to the aforementioned adequacy. An adequacy can either be evaluated by a data exporter or a public body and be established by unilateral recognition of the exporting country or by mutual recognition between exporting and receiving country. Within this category there are subcategories, which can be determined according to how this adequacy is applied and by whom. One subcategory looks at the data exporter side. It makes the transfer dependent on the data exporter having carried out a self-assessment of the data protection framework of the recipient country. A second subcategory is based on the perspective of a holder of sovereign rights, such as a SA. Adequacy is then established for a specific recipient country by an “adequacy decision”.

The European framework has a three-tier mechanism that falls into the category of a “flow conditional on safeguards” mentioned above. Its conditions for such transfers apply to both the recipient country and the data exporter. In the first case, the transfer can take place to countries with an “adequate level of protection”. In the second case, even when the recipient country is not deemed adequate, personal data can be transferred under appropriate safeguards (including BCR, SDPC, and certification mechanisms approved by the Union). Even when there are no adequacy decision and no appropriate safeguards in place, this mechanism still allows such transfers under certain conditions, namely if the data subject has given his or her explicit consent, if the transfer is occasional and is necessary in the context of a contract or in order to pursue legal claims, if the transfer is necessary for the protection of an important public interest laid down in Union law or in the law of a Member State, to protect vital interests of the data subject, or if the transfer is made from a public register.

The intent of Art. 38 PIPL is that the data controllers shall take necessary measures to ensure that the processing of personal data by overseas recipients meets the personal data protection standards stipulated in PIPL. Art. 38 PIPL indicates an intention to allow mutual recognitions with respect to TFPD.¹⁸⁸⁷ Greenleaf noted in this respect that PIPL’s approach

is to turn this into a negotiation with the CAC or other PRC authorities. This is consistent with the international engagement requirement that the state is to actively participate in the formulation of international rules for protecting personal information, and promote

¹⁸⁸⁶ Kuner, C. [Christopher]. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD iLibrary*, No. 187. <https://doi.org/10.1787/5kg0s2fk315f-en>. P. 20.

¹⁸⁸⁷ Art. 38(3) PIPL reads: “where it has concluded a contract with an overseas recipient according to the standard contract formulated by the state cyberspace administration, specifying the rights and obligations of both Parties.”

mutual recognition of rules and standards for the protection of personal information with other countries, regions, and international organizations (art. 12). When coupled with the allowance of data export provisions in treaties and agreements (art. 38, above), this seems to open the way for China to negotiate mutual data export agreements, multilateral or bilateral. It remains to be seen whether this approach will play a significant role in China's international engagements such as its application to become a party to the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), or in relation to the 165 countries that it has agreements with under its "Belt and Road Initiative".¹⁸⁸⁸

PIPL follows the GDPR in terms of other safeguards such as certain standardized contractual clauses and certifications through the Certification Specification and the Draft Standard Contract Provisions, both mentioned above¹⁸⁸⁹. The GDPR identifies clear derogations in its Chapter V, while Art. 38(4) PIPL leaves room for future interpretation.¹⁸⁹⁰

In the third, the "strictest" category of mechanisms, the focus lies also on a sovereign assessment through an adequacy recognition. The difference to the second category, however, is that if such an adequacy has not been established, a transfer can only be permitted by an ad hoc authorization of an authority. In the strictest form of all mechanisms – as a subcategory of this strict category – an adequacy recognition for a specific recipient country is not even provided for, but only an ad hoc authorization; all transfers, either generally all, those of a specific sector, or those of a specific data type, are then subject to a review by a relevant authority.

Although PIPL aligns with the GDPR, Chinese legislation as a whole still falls under this third category. In contrast to the GDPR, DSL, CSL and PIPL commit to security assessments for OCII to give authorities more control over such data types and sectors. The Chinese approach is "based on the central role of cybersecurity in national security and is, therefore, highly restrictive. [...] This was translated into an initial focus on data inflows regulations for national security and surveillance reasons, and also to increase interest in restricting outflows"¹⁸⁹¹. While Art. 38 PIPL does not explicitly determine the steps necessary for an adequacy recognition, this was fulfilled by the PRC Security Assessment Measures mentioned above¹⁸⁹². Although such an assessment (either PIPIA or CAC-led assessment) also examines many criteria of the legal framework of the recipient country, recognition within the scope of such an assessment does not result in the recipient country being deemed adequate as such, as is the case with an adequacy decision by the Commission. Rather, an "assessment passed" according to Art. 38(1) PIPL only results in the data transfers of the corresponding data controller being allowed (as long as the transfer also meets all other the personal data protection standards stipulated in PIPL). The requirements in Chinese law therefore have little in common with the adequacy approach of the GDPR, as Greenleaf correctly noted: "None of the conditions in article 38(2)(a)-(d) [Art. 38(1)-(4) PIPL] refer directly to the state of the law

¹⁸⁸⁸ Greenleaf, G. [Graham]. (1 October 2021). China's Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report, 2021*(172), <https://ssrn.com/abstract=3989775>. P. 5.

¹⁸⁸⁹ Chapter IV, Section IV.

¹⁸⁹⁰ Art. 38(4) PIPL reads: "Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department."

¹⁸⁹¹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 102.

¹⁸⁹² Chapter IV, Section IV.

in the receiving country, so conditional exports in China have little similarity to adequacy in the EU.”¹⁸⁹³ In addition to China, ten other countries fall into this third category.¹⁸⁹⁴

The mechanisms can also be categorized by the type of data flow restrictions. These can be distinguished according to whether no particular type is regulated, or local copy and/or local storage and/or local processing and/or local access is required. Here, it is important to note the peculiarity that a “complete prohibition on the transfer of data amounts to a *de facto* requirement for local storage and processing. By contrast, a local storage requirement does not always correspond to a complete prohibition of cross-border transfer”.¹⁸⁹⁵ Again, the transitions between the aforementioned levels of restrictiveness and types of restrictions are fluid. Also, the types of restrictions may fall within “general” or “sector specific” scopes. One reason for this is the domestic technical feasibility of data flow restrictions, especially for developing countries. UNCTAD noted in this respect that those countries “may not have adequate capacity to build high-quality, local digital platforms, and may thus better achieve economic development by adopting regulations that facilitate secure and privacy-compliant cross-border data transfers, such that local companies can access services provided by foreign digital platforms.”¹⁸⁹⁶

The first category of types of data flow restrictions, where there are no specific requirements, is the most commonly used. The GDPR and the Brazilian *Lei Geral de Proteção de Dados* (LGPD) do not require data flow restrictions. But the LGPD requires recipient countries to ensure an adequate level of data protection, to have approved legal mechanisms (such as model contract clauses) or to have data subjects’ consent. But “given the strict requirements in GDPR, there is no easy way for cross-border data flows, as few countries have been granted adequacy. Moreover, certain recent developments – such as the Data Governance Act, the decision of the European Court of Justice in *Schrems II*, as well as the GAIA-X initiative – may suggest that the European Union is shifting in its position on data localization”.¹⁸⁹⁷ The draft EUCS¹⁸⁹⁸ is also an example of this direction.

This *de facto* restriction is actually at odds with the stated objectives of the GDPR and also the Union’s position in the WTO, as the Commission had stated on the latter that

cross-border data flows shall not be restricted by: (a) requiring the use of computing facilities or network elements in the Member’s territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member; (b) requiring the localization of data in the Member’s territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member’s territory or upon localization requirements in the Member’s territory.¹⁸⁹⁹

¹⁸⁹³ Greenleaf, G. [Graham]. (1 October 2021). China’s Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report*, 2021(172), <https://ssrn.com/abstract=3989775>. P. 4.

¹⁸⁹⁴ According to UNCTAD, these countries have adopted some form of restrictive or guarded regulatory frameworks on transborder data flows: India, Indonesia, Kazakhstan, Nigeria, Pakistan, Russian Federation, Rwanda, Saudi Arabia, Turkey, Viet Nam. UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 137.

¹⁸⁹⁵ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 25.

¹⁸⁹⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 138.

¹⁸⁹⁷ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 107.

¹⁸⁹⁸ See Chapter II, Section II.3.8.2

¹⁸⁹⁹ WTO. *Communication from the European Union, Joint statement on electronic commerce, EU proposal for WTO disciplines and commitments relating to electronic commerce*, INF/ECOM/22, https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf, (26 April 2019). P. 4.

The second category contains a “local copy”, “local storage” or “local access” requirement, again with individual deviations in sub-categories. This type of restriction does not include a prohibition on transferring or storing copies of the personal data abroad if a copy of these data is saved domestically. The objective of this type is an easier access to this data for law enforcement purposes on domestic soil instead of an access to these data stored in another jurisdiction. The US requires that any company supplying cloud services to its Department of Defense must store its data only domestically.¹⁹⁰⁰ Other approaches establish that data be stored and made accessible to local authorities without prescribing the country where the data have to be stored.¹⁹⁰¹ Other countries require social media companies¹⁹⁰², personal data collected by public bodies,¹⁹⁰³ financial data,¹⁹⁰⁴ or domestic suppliers of telecommunications as well as Internet services,¹⁹⁰⁵ to store locally. When it comes to local servers on which this data must be stored, Vietnam takes a special path related to the infrastructure of this storage, “where any company that wants to process data is required to build at least one server in the country serving the inspection, storage, and provision of information at the request of competent state management agencies. Also in this case, the regime could easily turn into a local processing requirement if the server has to be used to process all information managed by the data controller or data processor”. A sub-category “relates to those where there are no flow restrictions but foreign storage is not allowed, implying that processing can occur abroad, but that post-processing, data must be returned to the home country for storage”¹⁹⁰⁶.

A third category requires that data be stored locally and this is combined with conditions attached to the possibility of transferring and processing those data abroad. These last two requirements can be related to a desire to encourage the development of domestic data storage and other data service industries and thus can be related to industrial policy objectives¹⁹⁰⁷ as well as to “nations seeking broader control over citizen activities”¹⁹⁰⁸. This category therefore adds a requirement for local processing on top of local storage. A data exporter “is therefore required for the company to either build a data center or to switch to local providers of data processing solutions. Alternatively, the company might decide to leave the market altogether. If this regime applies, the company can still send the data abroad, for example to the parent company, after the main processing.”¹⁹⁰⁹ All three pillars of China’s legislation related to the transborder transfer of persona data – CSL, DSL, and PIPL – impose restrictions on TFPD in certain situations.¹⁹¹⁰ PIPL requires that OCII store PI collected and generated within China. In addition to regulation for OCII, China

imposes several sector-specific data localization regulations, including for health information, information collected by credit investigation organizations, personal information collected by commercial banks, Internet map service organizations, personal information and business data collected by online taxi platform companies

¹⁹⁰⁰ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 100.

¹⁹⁰¹ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Para. 44.

¹⁹⁰² Turkey and Pakistan

¹⁹⁰³ Canada

¹⁹⁰⁴ Sweden, India

¹⁹⁰⁵ Vietnam

¹⁹⁰⁶ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Para. 45.

¹⁹⁰⁷ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Para. 45.

¹⁹⁰⁸ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 11.

¹⁹⁰⁹ Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*.

<https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>. P. 4.

¹⁹¹⁰ See Chapter IV, Section IV.

and Internet bicycle rental operators, and a general restriction on the cross-border transfer of State secrets.¹⁹¹¹

In Russia, explicit localization was applied in particular by Law No. 242-FZ¹⁹¹². This law requires operators, if personal data have been collected, and, as a result of a data processing (including previously collected personal data), actions provided for by Art. 18 of Law 152-FZ¹⁹¹³ have been commenced, to ensure that the recording, systematization, accumulation, storage, adjustment (update, alteration), and retrieval of personal data of citizens of the Russian Federation will be performed through database servers located in the territory of the Russian Federation. We agree therefore with Tomiura, Ito and Kang, who found that Russia, China [...] are countries, which “require firms to locate certain categories of data (categories wider than personal data) within the host countries”¹⁹¹⁴. Similarly, Kenya, India and Pakistan prohibit transborder transfers of “critical personal data” or personal data based on “grounds of strategic interests of the state or protection of revenue” and require that such data be stored and processed locally.¹⁹¹⁵ Other countries “impose strict localization requirements for specific data categories, including health, defense, IoT, and mapping data and, more broadly, for critical government and public data. Other examples of strict localization requirements relate to business records, tax records and accounting records.”¹⁹¹⁶

There is theoretically another, fourth, category. This concerns a local storage, local processing and local access requirement, which results in a ban on transfers, where the data exporter is not allowed to even send a copy of the personal data abroad. However, Ferracane found that

to date, there is no country that imposes an economy-wide ban on the transfer of all data abroad, regardless of the nature of the data. However, some jurisdictions impose bans on the transfer of specific sets of data. For example, Australia requires that no personal electronic health information is held or processed outside national borders. Another example is two provinces of Canada (British Columbia and Nova Scotia) which have enacted laws that require personal information held by public institutions (such as schools, universities, hospitals or other government-owned utilities and agencies) to stay in Canada - with only a few limited exceptions.¹⁹¹⁷

The transfer mechanisms can therefore be summarized as follows:

¹⁹¹¹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 102.

¹⁹¹² Russian Federation, State Duma. *Federal Law No. 242-FZ of 21 July 2014 Amending Certain Legislative Acts of the Russian Federation as to the Clarification of the Processing of Personal Data in Information and Telecommunications Networks*, <https://wilmap.stanford.edu/entries/federal-law-no-242-fz>, (21 July 2014).

¹⁹¹³ Russian Federation, State Duma. *Federal Law No. 152-FZ of 27 July 2006 On Personal Data*, https://wko.at/ooe/Branchen/Industrie/Zusendungen/FEDERAL_LAW.pdf, (27 July 2006).

¹⁹¹⁴ Tomiura, E. [Eiichi] and Ito, B. [Banri] and Kang, B. [Byeongwoo]. (14 March 2020). *Cross-border data transfers under new regulations: Findings from a survey of Japanese firms*. <https://voxeu.org/article/cross-border-data-transfers-under-new-regulations>.

¹⁹¹⁵ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 125.

¹⁹¹⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 126.

¹⁹¹⁷ Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>. P. 4.

Framework	Scope of application	Level of restrictiveness	Type of data flow restriction
Europe	General	Conditional on safeguards (prescriptive)	No specific type
US	Sector specific	Ex-post accountability (light touch)	Local storage requirement
China	Sector specific and data type specific	Ad-hoc authorization (restrictive/guarded)	Local storage, local processing and local access requirement

1.4.2. Regulatory cooperation

Regulatory cooperation “comprises intergovernmental efforts for best practice and common normative principles” and can also be divided into universal and limited.¹⁹¹⁸ Convention 108+ and the CCC are to date the only binding international agreements on legal harmonization for data protection and law enforcement. Limited approaches include rules with regional reach that exist for the European Union as well as for APEC and ASEAN economies. ASEAN set rules for regulatory cooperation in its Framework on Digital Data Governance. Paras. 40ff. of the APEC Privacy Framework 2015 describe in detail how cooperation should be fulfilled. The European Union does so in even greater detail. Principles and guidelines have been developed by the OECD and the UN that promote harmonization of national regulations among its members in this area, e.g., in paras. 20-23 of the OECD Guidelines 2013. Various MLATs¹⁹¹⁹ provide legal assistance against illegal activities that originate in another jurisdiction.

1.4.3. Technical standards

Regulatory issues are often resolved through purely technical standardization. This can have universal character and then takes place in multi-stakeholder forums. These include ISO/IEC standards, the Institute of Electrical and Electronics Engineers (IEEE), and the World Wide Web Consortium (W3C). However, technical standards can also be limited in scope, for example by national and supranational standard setting, by exclusive data spaces (e.g., European Cloud) or bilateral agreements or equivalence decisions (e.g., Digital Economy Agreement between Australia and Singapore).

1.4.4. International trade rules

TFPD are affected by WTO rules, the applicability of which has already been discussed above¹⁹²⁰. The reason this is the world’s only universal trade-related approach is that, as Geist noted¹⁹²¹, that “trade agreements invariably involve trade-offs on a wide range of issues from tariffs on agricultural goods to environmental policy. The inclusion of data governance as a trade-related issue complicates the policy process since it treats a critical yet complex policy matter as little more than a trade bargaining chip”. This complexity naturally increases the more Member States, the more stakeholders and their

¹⁹¹⁸ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 15.

¹⁹¹⁹ See Chapters II-VII

¹⁹²⁰ Chapter V, Section III.

¹⁹²¹ Geist, M. [Michael]. (4 April 2018). *Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. A CIGI Essay Series on Data Governance in the Digital Age*. https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security/?utm_source=twitter&utm_medium=social&utm_campaign=data-series.

interests are involved, and therefore the more trade-offs have to be made. This is exemplified by the diverging goals of the Member States during a WTO Ministerial Conference.

Proposals for incorporating free cross-border data flows in the WTO regime were, however, opposed by some developing country members – such as India, Indonesia and South Africa – and by the African Group. These members expressed concerns that binding rules on cross-border data flows would limit the policy space for those countries to adopt data and digital policies that could help their economies achieve industrialization and technological development. [...] Germany and France [...] expressed concerns about a commitment to the free flow of data.¹⁹²²

The WTO JSI process regarding e-commerce can basically be classified as a universal approach, but it has one limitation. As UNCTAD also stated, there was a “limited participation” in this process for the aforementioned reason and others. Also, some countries claimed that “these flows are already covered by existing agreements and commitments (such as GATS Mode 1)”¹⁹²³. This is correctly also due to the fact that “insufficient knowledge about the issues at stake, including those beyond the trade domain” exists, and “views on this matter diverge widely, and have a strong political component”¹⁹²⁴.

Limited approaches to trade rules are trade commitments that regulate data flow, localization prohibition, and source code access disciplines. Examples include TiSA¹⁹²⁵, and – from the APAC framework¹⁹²⁶ – USMCA, CPTPP, RCEP, and NAFTA.

1.5. Maturity

The frameworks can also be distinguished by their so-called “maturity”. For the purposes of this thesis, maturity is understood as the stage at which all data protection measures taken so far are in place. These measures include not only data protection laws within a framework, but also other elements accompanying them, as the following graphic illustrates.

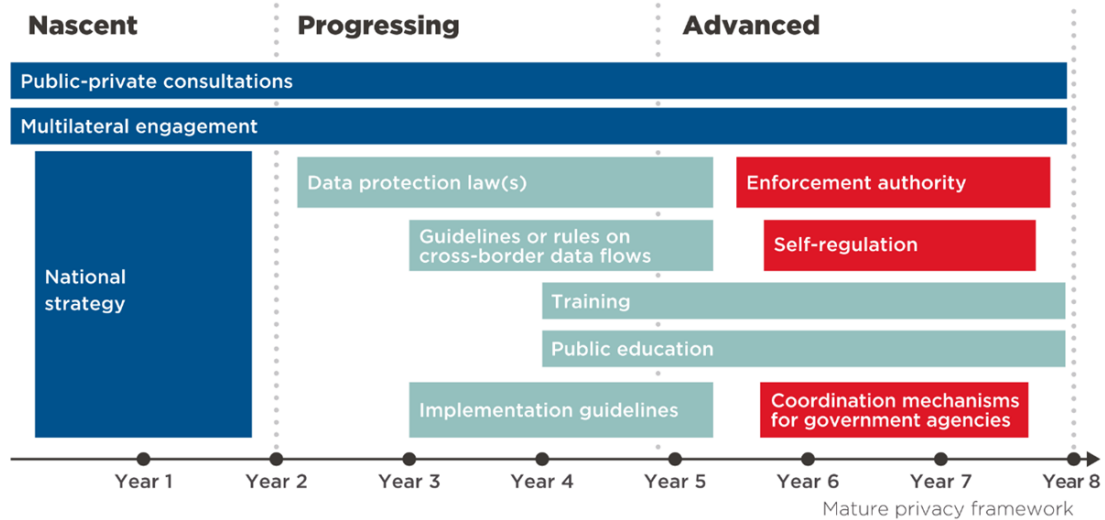
¹⁹²² UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 149.

¹⁹²³ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 150.

¹⁹²⁴ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 150.

¹⁹²⁵ See Chapter VIII, Section I.1.

¹⁹²⁶ See Chapter IV, Section III.



Source: GSMA, "Roadmap of privacy elements"¹⁹²⁷

Since maturity is determined by the entirety of a framework, it also includes elements that may have already been analyzed in Chapter IX Section III.1.1.-1.4. In this respect, Chapter IX Section III.1.5 also forms a "catch basin" for such elements that have not yet been dealt with.

De Terwangne¹⁹²⁸ separated five global models of data protection:

- "Comprehensive Model": A general law that governs the processing of personal data by both the public and the private sector. Compliance is ensured by an oversight body.
- "Patchwork Model / Piecemeal Model": A fragmented system of protection, consisting in various measures as sector-orientated, specific addressed or on arising problems focused regulations.
- "Sector-orientated Model": Rules in favor of specific laws, governing specific technical applications, or specific technical applications, or specific regions, such as financial data protection.
- "Model of self-regulation": Companies and industry establish codes of conduct or practice and engage in self-policing.
- "Risk-Burden Balance Model": Legislation exempts ranges of activities, considering them as not dangerous for data protection issues of data subjects.

This suggests that the highest maturity can be achieved by a comprehensive model. However, the five models mentioned above are not the only decisive factors for achieving a certain maturity. At least in theory, it is possible to achieve the same number of elements of the GSMA classification mentioned above with a self-regulatory approach to data protection. In the considerations in Chapters III and IV, State-level data protection laws in the US and China were mentioned several times and found to be "comprehensive" in themselves. However, this does not directly lead to a framework as a whole becoming comprehensive.

¹⁹²⁷ GSMA. (September 2018). *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC can Protect Data and Drive Innovation*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf. P. 5.

¹⁹²⁸ de Terwangne, C. [Cécile]. (2009). Is a Global Data Protection Regulatory Model Possible?. In S. [Serge] Gutwirth and Y. [Yves] Pouillet and P. [Paul] De Hert and C. [Cécile] de Terwangne and S. [Sjaak] Nouwt (eds.), *Reinventing Data Protection?* (pp. 175–189). Springer. P. 179–180.

We agree with the determination of the first four models. A risk-based approach had been (partially) integrated even into the first data protection law in the world in 1970¹⁹²⁹, continued to be integrated in the Directive 95/46¹⁹³⁰, and is also integrated into some currently valid regulations (e.g., the GDPR¹⁹³¹ and the OECD Guidelines 2013¹⁹³²). However, whilst a purely Risk-Burden Balance Model was still present in the past by, e.g., excluding legal entities processing a small number of data subject's personal data from data protection obligations,¹⁹³³ this model has disappeared to this day. This is probably because nowadays, the vast majority stakeholders in the global ecosystem of transborder data flows have recognized that the activities not endangering data protection issues of data subjects have become negligible.

The European framework, therein in particular the GDPR, is one of the most comprehensive models for data protection in the world,¹⁹³⁴ and clearly at advanced level.

While the GDPR guarantees comprehensive data protection, there is no such law at US federal level.¹⁹³⁵ The reason lies in the US' perception of democratic governance, the responsibility of the State to protect the rights of its citizens, and the effectiveness and equity of markets. The US' approach reflects a "basic distrust of government; markets and self-regulation rather than government oversight shape information privacy in the US and as a result the legislation that does exist is reactive and issue-specific; protection tends to be tort-based and market orientated rather than legislative or regulatory"¹⁹³⁶. The selective regulatory approach reflects the greater reluctance in the US to intervene by regulating the relationship between private individuals. Therefore, the US approach often only reacts to specific ad hoc concerns. Instead of a comprehensive model, there is a "patchwork" of State level data protection laws, with no federal law yet in place. The overall approach to data protection in the US is "is complex, associating federal and state level regulations and self-regulatory and co-regulatory measures"¹⁹³⁷ and "omnibus legislative solutions are eschewed with respect to the private sector"¹⁹³⁸. US laws are on the one hand only sector specific. This includes for example health, financial privacy, education records, telephone consumer protection, children's privacy online, and cable communications. On the other hand, the US addresses only specific and sometimes narrowly targeted privacy issues. There is therefore an overlap between the

¹⁹²⁹ *Bundesland Hessen. Datenschutzgesetz*, Gesetz- und Verordnungsblatt für das Land Hessen, GVBl. II 300-10, 1 Y 3228 A, 625–628, (7 October 1970). Gellert found in his analysis of this "Data Protection Law" that it "implicitly frames data protection as a risk regulation regime since one of its purposes is to safeguard the constitutional structure of the state [...] against all risks entailed by automatic data processing". Gellert, R. [Raphaël]. (2015). Data protection: a risk regulation? Between the risk regulation of everything and the precautionary alternative. *International Data Privacy Law*, 5(1), 3–19. Oxford University Press. P. 5.

¹⁹³⁰ "the risks represented by the processing" (Art. 17 Directive 95/46), "specific risks to the rights and freedoms of data subjects" (Art. 20 Directive 95/46), and the proportionality test (Art. 7(f) Directive 95/46).

¹⁹³¹ "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.", Art. 24(1) GDPR.

¹⁹³² "which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties.", Art. 2 OECD Guidelines 2013.

¹⁹³³ The Australian Privacy Act 1988 exempted all small businesses from respecting national privacy principles, and in Japan, entities that have been holding personal data on less than 5,000 individuals or for less than 6 months were exempted from regulation. See de Terwangne, C. [Cécile]. (2009). Is a Global Data Protection Regulatory Model Possible?. In S. [Serge] Gutwirth and Y. [Yves] Pouillet and P. [Paul] De Hert and C. [Cécile] de Terwangne and S. [Sjaak] Nouwt (eds.), *Reinventing Data Protection?* (pp. 175–189). Springer. P. 180.

¹⁹³⁴ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 104.

¹⁹³⁵ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 100.

¹⁹³⁶ Kobrin, S. [Stephen]. (2004). Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 30(1), 111–131. P. 115.

¹⁹³⁷ de Terwangne, C. [Cécile]. (2009). Is a Global Data Protection Regulatory Model Possible?. In S. [Serge] Gutwirth and Y. [Yves] Pouillet and P. [Paul] De Hert and C. [Cécile] de Terwangne and S. [Sjaak] Nouwt (eds.), *Reinventing Data Protection?* (pp. 175–189). Springer. P. 179.

¹⁹³⁸ Bygrave, L. A. [Lee A.]. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press. P. 191.

piecemeal/patchwork-model and the sector-orientated model in the US framework. The US approach was therefore also called “relatively atomized”¹⁹³⁹, a “patchwork of rules”¹⁹⁴⁰ or a model that deals with data protection in specific sectors and problems in a “haphazard manner”¹⁹⁴¹.

An adoption of ADPPA could potentially bring the US framework closer to an advanced level (according to the GSMA classification) and a comprehensive model (according to the de Terwangne classification). This requires a section-by-section analysis of this proposed Act, with data protection principles and essential guarantees to be addressed in detail in Chapter IX Sections III.2 and III.3 The scope of ADPPA could result in

many organizations in the health care sector, education sector, and financial services sector would not be required to comply with the law in regard to much, if not all, of the data they hold (see discussion below). Further, some small businesses that do not engage in interstate commerce could fall outside of the FTC’s jurisdiction and, therefore, would be exempt from the law. In addition, certain organizations with annual revenues of USD 41 million or less would not be required to comply with some aspects of the law in accordance with the small data exception [Section 209(c)].¹⁹⁴²

“Covered data” in ADPPA is defined as in the GDPR, but with three differences. First, ADPPA would not cover employee data (Sec. 2(8)(B)(ii)), and second, would exclude “publicly available information” from the material scope (Sec. 2(8)(B)(iii)), whereas the GDPR also considers this to be personal data in scope, but privileges those data types through derogations. Last, the term “de-identified data” (Sec. 2(8)(B)(i)) is more in line with the European counterpart of “pseudonymization”. This could render some safeguards ineffective, as data aggregated from multiple data sources often still allow inference to an individual and re-identification. ADPPA also explicitly includes – as a special feature compared to the GDPR – “derived data”, which is “collected data that results from the derivation of information, data, assumptions, or inferences from facts, evidence, or any other source of information or data about a person or device.” Sec. 2(28) regulates “sensitive covered data,” encompassing all types of sensitive personal data as the GDPR; in addition to these, “government-issued identifier”, “private communications of the individual”, “login credentials”, “online activities data” und “private use data”¹⁹⁴³ are classified as such. Covered data processing activities are defined similarly to the GDPR, with ADPPA distinguishing between the main processing steps of “collection”, “processing”, and “transfer”. Collection means “acquiring covered data by any means. Processing means any operation or set of operations performed on covered data. Transferring means to disclose, make available, or license covered data by any means or in any way. Together, these terms dictate the actions of covered legal entities and individuals with respect to covered data.”¹⁹⁴⁴ However, covered data subject to licensing is unknown to the GDPR.

¹⁹³⁹ Bygrave, L. A. [Lee A.]. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press. P. 191.

¹⁹⁴⁰ Kobrin, S. [Stephen]. (2004). Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 30(1), 111–131. P. 115.

¹⁹⁴¹ Roch, M. P. [Michael P.]. (1996). Filling the Void of Data Protection in the United States: Following the European Example. *Santa Clara Computer and High Technology Law Journal*, 12(1), 71–96. P. 93.

¹⁹⁴² Manatt, Phelps & Phillips LLP. (15 June 2022). *Congress Releases Draft American Data Privacy and Protection Act*. <https://www.jdsupra.com/legalnews/congress-releases-draft-american-data-6894033>.

¹⁹⁴³ Which includes calendar, address book, phone and text logs as well as audio and video recordings. This seems to aim include the data usually processed during services of platforms such as WhatsApp and Facebook into the “sensitive information” category of ADPPA.

¹⁹⁴⁴ USA, Senate Committee on Commerce, Science, and Transportation. *American Data Privacy and Protection Act Draft Legislation. Section by Section Summary*, <https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50>, (2022). P. 1.

ADPPA differentiates between the roles of a “covered entity” (corresponding to the role of a controller under the GDPR), “service provider” (corresponding to the role of a processor under the GDPR), and “third Parties” (similar to a controller which receives personal data from another controller under the GDPR) being subject to ADPPA. Federal, State, Tribal, territorial, or local government entities are not covered by ADPPA, Sec. 2(9)(B)(i) ADPPA. Sec. 2(21) defines “large data holders” and is similar to the European Data Strategy’s VLOPs. This, however, does not reach the comprehensive level of the GDPR, because “ideally, privacy rules should apply equally to all organizations regardless of size – privacy risks to consumers depend on the sensitivity of the data and the context of its collection, not the size of the organization collecting the data.”¹⁹⁴⁵ An entity that controls or is controlled by or is under common control with another covered entity is included by the term covered entity, Sec. 2(9)(A)(ii) ADPPA. Therefore, ADPPA does not distinguish as strictly as the GDPR between the various legal entities belonging to the same group, but rather takes the group as a whole into account.

This is also made clear by the term “third party”, which does not include a legal entity that processes covered data which it has received from an affiliate unless one of the entities involved is a large data holder, Sec. 2(35)(B) ADPPA. This may result in a privilege for data transfers within a group of companies, a concept that is different to the GDPR where data transfers within a group of companies are subject to the same legal requirements as transfers to external Parties. “Individual” refers to the person who the covered data relates to, so it is comparable to the data subject of the GDPR. However, the term covers only those that reside in the US, Sec. 2(16) ADPPA. Consequently, individuals residing in the EU shall not enjoy the protection of ADPPA when their personal data will be processed by covered legal entities.

ADPPA would allow data subjects to opt out of data processing in general (instead of requiring them to opt in). ADPPA requires affirmative express consent which must be freely given, specific, informed, and unambiguous for an act or practice that is clearly communicated in response to a specific request from a covered entity, Sec. 2(1)(A)-(C) ADPPA. These requirements largely correspond to the requirements of a valid consent under the GDPR. The FTC is even called upon to develop “centralized opt-out mechanisms”, which would allow data subjects to opt out of all covered data processing if the FTC determines that such mechanisms are feasible. ADPPA specifies even more precisely than the GDPR that not only “plain language” is required, but information in the language of a product or service provided to the data subject. However, affirmative express consent is only required for a few data processing activities, including transfers of sensitive covered data to third Parties, Sec. 102(a)(3)(A) ADPPA. Most of the obligations established by ADPPA are directed at the covered entity, but certain obligations also on service providers as well as third Parties when they process covered data. Information obligations under Sec. 202(b) ADPPA largely correspond to those required under Arts. 13-14 GDPR. ADPPA would also provide for the implementation of reasonable data security practices and allows those meeting other federal privacy laws.

The FTC and the State attorneys general would be entrusted with ADPPA’s enforcement, which would add minimum fifty new enforcement agencies through the Attorneys General Offices, Sec. 401, 402. The FTC would establish a new bureau comparable in structure, size, organization, and authority to the existing Bureaus to exercise its authority under the bill, Sec. 401. The FTC would also develop a public database of data traders and establish a mechanism for data subjects to opt out. Also, the FTC would be

¹⁹⁴⁵ Castro, D. [Daniel]. (13 June 2022). *A Review: The American Data Privacy and Protection Act*. <https://www.govtech.com/policy/a-review-the-american-data-privacy-and-protection-act>.

charged with, among other things, to “include additional categories of covered data within the sensitive covered data definition where those categories require similar protection as a result of new methods for collecting or processing covered data”, to “issue guidance to help establish what is reasonably necessary, proportionate, and limited”, and to provide guidance and consultation to covered legal entities regarding compliance with the ADPPA.¹⁹⁴⁶ This fulfills the elements of a “coordination mechanism for government authorities” and the “implementation guidelines”. The draft also requires a data protection officer. The “self-regulation” element would also still play a role in ADPPA, as “ADPPA would require data brokers to register with the FTC and allow third-party audits of how data brokers share information with others” and “establish a process for organizations to submit technical compliance programs for the agency’s approval”¹⁹⁴⁷. The elements of “training” and “public education”, however, are not mentioned under the proposed ADPPA. Overall, this federal bill would draw upon many of the European frameworks’ elements and could be considered as “advanced”. However, since there is no regulation for the public sector, the US framework as such is not yet a comprehensive model. The question of whether ADPPA would encompass all data subjects’ rights, principles and essential guarantees known to the GDPR is analyzed in more detail below.¹⁹⁴⁸

At US State level, the CPRA drives significant improvement for the rights and freedoms of California data subjects. As noted above¹⁹⁴⁹, the CPRA achieves, once effective on 1 January 2023, a comprehensive level approaching that of the European framework. Nevertheless, a DPO remains an unknown instrument to the CPRA and therefore omits an important element for the further progress of its maturity. In contrast to European framework, CCPA and CPRA do not presuppose the adequacy of foreign data protection regimes alike Arts. 44 ff. GDPR. The transfer of personal data from California to the EU – unlike from the EU to the US – is not subject to any special legal requirements. CCPA and CPRA are nevertheless a further step towards alignment with the GDPR, which could then make it easier for the Commission to issue a positive adequacy decision on the State of California.¹⁹⁵⁰

¹⁹⁴⁶ USA, Senate Committee on Commerce, Science, and Transportation. *American Data Privacy and Protection Act Draft Legislation. Section by Section Summary*, <https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50>, (2022). P. 1–2.

¹⁹⁴⁷ Castro, D. [Daniel]. (13 June 2022). *A Review: The American Data Privacy and Protection Act*. <https://www.govtech.com/policy/a-review-the-american-data-privacy-and-protection-act>.

¹⁹⁴⁸ Chapter IX, Section III.2.; and Chapter IX, Section III.3.

¹⁹⁴⁹ Chapter III, Section II.2.; and Chapter IX, Section II.2.

¹⁹⁵⁰ The GDPR specifically refers in Art. 45(1) to the possibility of a “territory” or “one or more specific sectors” obtaining an adequacy decision, which contemplates subnational adequacy decisions.



Source: IAPP, “Enacted State Comprehensive Privacy Laws”¹⁹⁵¹

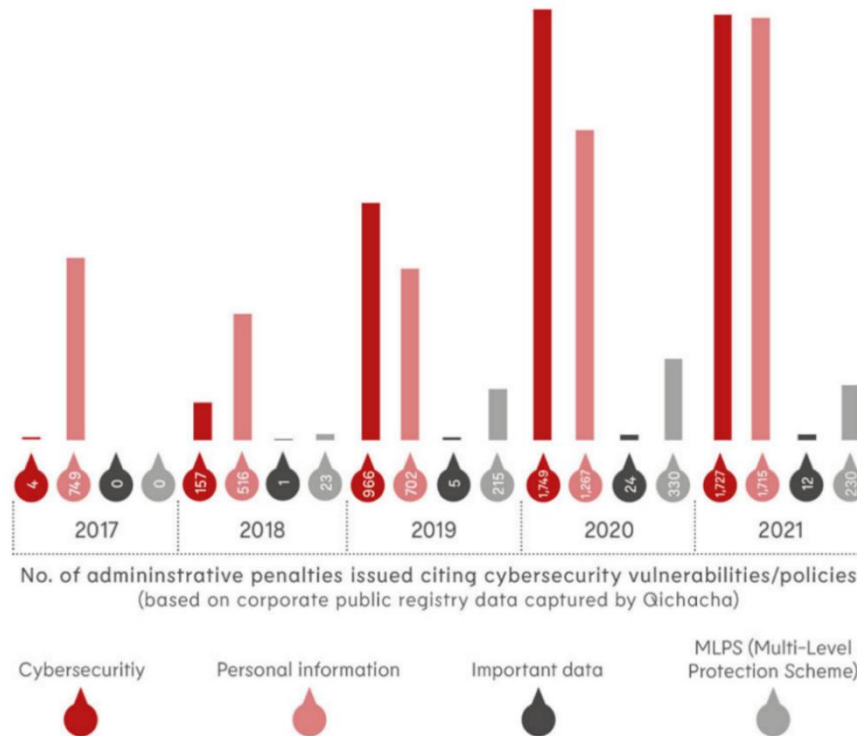
ASEAN Member States’ regulation on data protection are divided into comprehensive models and sector-orientated models. The former include: Malaysia, Philippines, Singapore, Thailand. Sectoral regulation is found in Laos, Cambodia, and Indonesia. In Indonesia, Indonesia’s House of Representatives passed in September 2022 the “Personal Data Protection Bill”, which would be a comprehensive regulation and, for the most part, resemble the GDPR. Vietnam has regulations in place that are scattered throughout different pieces of legislation. Brunei and Myanmar have no specific law governing personal data in place. The ASEAN Framework on Digital Data Governance includes the elements “guidelines or rules for cross-border data flows” and “implementation guidelines,” but omits the elements “training” and “public education.”

Although the level of data protection established in APEC by the APEC Privacy Framework 2015 is lower than that of the GDPR, cooperation through different policy papers in APEC has raised the maturity of the framework. CPEA created a legal framework for the voluntary cooperation of public bodies in the APEC countries. Any APEC economy that has a Privacy Enforcement Authority can participate in CPEA. Although non-binding, it has a supportive influence on the official exchange of information in the event of data protection violations and forms an important building block for the establishment of the CBPR-System. The actual success of the CBPR system in practice remains to be seen, as to date only eight APEC Member States participate.

Through the enactment of new regulatory instruments in the last three years, there are increasing parallels from the Chinese approach to those of the OECD and the European frameworks. Similarities to the GDPR include particularly consent, but also the exercise

¹⁹⁵¹ Desai, A. [Anokhy]. (7 July 2023). *US State Privacy Legislation Tracker*. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker>.

of data subject rights, technical organizational requirements for data security, and sanctions for violations. The following graphic shows that the enforcement of these regulations has become increasingly strong.



Source: Sinolytics GmbH, "China's cyber and data regulations: Maturing framework, increasing enforcement"¹⁹⁵²

Nevertheless, there are still differences with the GDPR.

There are no objective criteria for consent to export, no role for an independent Data Protection Authority (the PIPL does not provide for one), and no provisions for data controllers to appeal to a court against a CAC decision. CAC control over the above conditions (a)-(d) [Art. 38(1)-(4) PIPL] amounts to CAC discretion to prohibit some categories of export completely.¹⁹⁵³

As Greenleaf further noted, "unfettered government discretion to prohibit export of unspecified categories of personal data, such as the CAC can be argued to have, is one of the types of data localization about which its opponents (including advocates of the free flow of personal data) that accept conditional restrictions) have the highest concerns."¹⁹⁵⁴

Moreover, the Privacy by Design principle, as included in Art. 5 GDPR, is not found in PIPL. Lastly, even in theory it is difficult to understand the differently regulated processings of personal data and their demarcation between personal data processed by OCII, ordinary data, important data and core data; in practice at the latest, this might lead to problems in applying the law. The European framework tends to be framed in

¹⁹⁵² Sinolytics GmbH. (11 July 2022). *China's cyber and data regulations: Maturing framework, increasing enforcement*. https://sinolytics.de/sinolytics_weekly.

¹⁹⁵³ Greenleaf, G. [Graham]. (1 October 2021). China's Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report, 2021*(172), <https://ssrn.com/abstract=3989775>. P. 4.

¹⁹⁵⁴ Greenleaf, G. [Graham]. (1 October 2021). China's Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report, 2021*(172), <https://ssrn.com/abstract=3989775>. P. 4.

separate laws, whereas in China, a clear separation is not always made and a “standards regime” has been created, which is composed of an

interlocking system of laws, regulations, and standards [which] create a maze of rules spanning data, online content, and critical infrastructure. [...] In Chinese law, there is a mixture of data protection and data security regulations and many overlapping technical standards. Inside some regulations lies a duplication of content, the legislative background of which is still unclear. China uses vague language in standards, like in many Chinese laws and regulations, to avoid issues, such as World Trade Organization (WTO) challenges, while allowing the government maximum flexibility and discretion to apply onerous provisions when it sees fit.¹⁹⁵⁵

Greenleaf similarly noted that “there are many ways in which the data export, data localization, extra-territorial, retaliatory and platform provisions can be utilized to further the PRC’s foreign policy objectives”.¹⁹⁵⁶ Overall, the maturity of the Chinese approach is, through PIPL being effective, a “modern and sophisticated data privacy law, influenced by many advanced aspects of the GDPR, and which in a few respects may be stronger than the GDPR”¹⁹⁵⁷. Thus, PIPL could be considered as being of comprehensive nature, but the maturity of the whole Chinese system – although considered advanced on paper – does not yet reach the level of the European framework.

In the APAC framework, it is noticeable that it is moving towards the advanced level of the GSMA classification. APEC countries have achieved a high level of coordination mechanisms for government agencies through the CPEA, which is not always achieved by the European framework SAs due to the problems described in Chapter IX Section II.3.

Overall, the APAC framework is still, although at the step between progressing and advanced level, a sector-orientated model regarding the regulation of TFPD, which is why Hogan Lovells

recommend an approach to cross border transfer agreements that mandates a reasonable high water mark level of compliance that reflects mandatory requirements in most jurisdictions with comprehensive data protection laws, leaving room for specific treatment of transfers from jurisdictions with requirements exceeding this standard. This contracting structure avoids over-compliance and tailors the Parties’ legal obligations to the specific commercial context.¹⁹⁵⁸

The international organizations framework contains guidelines¹⁹⁵⁹ and thus “data protection laws” in the sense of the GSMA classification. Implementation guidelines are set out in para 19 of the OECD Guidelines 2013. Training and education are mentioned in para. 15(a)(i).

GPEN¹⁹⁶⁰ within the OECD fosters international co-operation among enforcement agencies, reflects a commitment by Member States to improve their enforcement

¹⁹⁵⁵ Sacks, S. [Samm]. (7 March 2019). *Testimony on “China: Challenges to U.S. Commerce, A Hearing Before the Senate Committee on Commerce, Science, and Transportation’s, Subcommittee on Security*. <https://www.commerce.senate.gov/services/files/7109ED0E-7D00-4DDC-998E-B99B2D19449A>. P. 2–3

¹⁹⁵⁶ Greenleaf, G. [Graham]. (1 October 2021). China’s Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report, 2021*(172), <https://ssrn.com/abstract=3989775>. P. 6.

¹⁹⁵⁷ Greenleaf, G. [Graham]. (1 October 2021). China’s Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report, 2021*(172), <https://ssrn.com/abstract=3989775>. P. 6.

¹⁹⁵⁸ Hogan Lovells. (26 January 2022). *ASEAN Launches Model Contractual Clauses for Cross Border Data Transfers*. <https://www.jdsupra.com/legalnews/asean-launches-model-contractual-6923372>.

¹⁹⁵⁹ See Chapter V

¹⁹⁶⁰ See Chapter V, Section I.3.

systems and laws, and can therefore be considered as a “coordination mechanism for government agencies” under the GSMA classification. However, due to the non-binding nature of these guidelines, there is no independent and neutral government agent tasked with ensuring adherence of the guidelines within this framework. Overall, this framework is therefore at progressing level and a self-regulatory model.

Main parts of a data-driven economy, namely Open Data, Big Data, Industry 4.0 and AI, are reflected in approaches to governing personal data. Within the GSMA classification, these (sub)strategies are components of a “national strategy”, which includes a “goal setting and a coordinated approach across government agencies, initiatives, and compatibility with related policies”¹⁹⁶¹. As mentioned above¹⁹⁶², the goal should be a whole-of-government approach to avoid silo solutions, because uncoordinated partial strategies could increase the regulatory challenge. Carvalho / Kazim similarly underlined this:

Data strategy in parallel/in situ with AI, blockchain and IoT strategy: as we have raised on several occasions, we read “data” strategy as part of broader concept of digital strategy, which includes digital transformation and the utilization of all novel computer science-based technologies (AI, blockchain, IoT, etc.). It appears the current thinking is sequential, where there is digital transformation, followed by a data strategy, after which perhaps AI strategy will proceed. The disadvantage of this is that the full potential benefits of the benefits of those subsequent technologies will be severely curtailed because of not fully incorporating them into the thinking of the data strategy. For example, the debate about standardization should be fully informed and premised on the idea that the standards will facilitate IoT, AI technologies, etc.¹⁹⁶³

In the future, this will determine the maturity of a framework even more significantly, also because “while many countries have open data strategies for government-funded or public data, most countries have not yet figured out how to ensure that when data is mined, personal data is protected, and firms do not exploit personal data, leading to problems such as identity theft, manipulative marketing or discrimination.”¹⁹⁶⁴ At this point, therefore, the approach of the various frameworks must be considered separately regarding a consistent strategy. The European Union¹⁹⁶⁵ and the US¹⁹⁶⁶ issued a variety of strategy policies on data governance acknowledging the importance of data to their economic development and national security. China has been working on defining its own strategy, which is currently in progress.

¹⁹⁶¹ GSMA. (September 2018). *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC can Protect Data and Drive Innovation*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf. P. 33.

¹⁹⁶² Chapter IX, Section I.2.1.

¹⁹⁶³ Carvalho, G. [Graca] and Kazim, E. [Emre]. (2022). Themes in data strategy: thematic analysis of 'A European Strategy for Data' (EC). *AI and Ethics*, 2(2), 53–63. P. 54.

¹⁹⁶⁴ Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 3.

¹⁹⁶⁵ See Chapter II, Section II.3.8.

¹⁹⁶⁶ USA, Office of Management and Budget. (2023). *Overview. Components of the Federal Data Strategy*. <https://strategy.data.gov/overview>. // USA, The White House. *Federal Big Data Research and Development Strategic Plan*, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/NSTC/bigdatardstrategicplan-nitrd_final-051916.pdf, (May 2016). // USA, National Institute of Standards and Technology. *Framework for Cyber-Physical Systems: Volume 1, Overview*, <https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview>, (26 June 2017).

Strategy type	China	European Union	US
Open Data Strategy		Public Sector Information Directive (2003), Data Strategy (2020), Open Data Directive, Data Act	Federal Data Strategy (2019) and Action Plans 2020/2021, Action Items 5 and 6
Big Data Strategy	Outline of Actions to Promote Big Data Development (2015) 13th five-year plan (2016) National Big Data Strategy (in progress)	Big Data Action Plan and Roadmap (2014), Data Strategy (2020)	Federal Big Data and Development Strategic Plan (2016)
AI Strategy	A Next Generation Artificial Intelligence Development Plan (2017), Three-Year Action Plan to Promote the Development of New-Generation Artificial Intelligence Industry (2017)	Communication on Artificial Intelligence (2018), White Paper on Artificial Intelligence (2020), Data Strategy (2020), Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (2020), Coordinated Plan on Artificial Intelligence (2021), Proposal for a Regulation laying down harmonized rules on artificial intelligence (2021), Communication on Fostering a European approach to Artificial Intelligence (2021)	Federal Data Strategy (2019) and Action Plans 2020/2021, Action Item 8, Blueprint for an AI Bill of Rights (2022)
Industry 4.0 / Manufacturing 4.0 / IoT Strategy	Made in China 2025 (2015)	Digitizing European Industry (2016), Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (2020), Data Strategy (2020)	NIST Framework for Cyber-Physical Systems (2017), Internet of Things Cybersecurity Improvement Act (2020)

1967

The three frameworks cover all sub strategies of a national data strategy – with two deviations. An Open Data Strategy is still lacking in China, although the Chinese government wants to share some of the data resources in the hands of government departments with the public, but also to offer some for paid, conditional use by companies. In the US, a federal IoT strategy exists only with a focus on cybersecurity and not as a holistic approach including data protection; it is thus a “piecemeal, leaving states and municipalities to enact their own laws and protections. Certain measures have focused on ensuring appropriate cybersecurity protocols are in place when governments deploy IoT devices, to guard against threats to public infrastructure and systems”¹⁹⁶⁸.

¹⁹⁶⁷ The colors of the tables that follow from here on mean: Green = fulfilled. Orange = partially fulfilled. Red = Not fulfilled.

¹⁹⁶⁸ New York City Mayor’s Office of the Chief Technology Officer. (2021). *IoT Strategy*. https://www1.nyc.gov/assets/cto/downloads/iot-strategy/nyc_iot_strategy.pdf. P. 27.

These two deviations may be since domestic stakeholder interests are particularly strong in these two fields and complicate developing a comprehensive strategy; in China, this is the stakeholder “State”, in the US the stakeholder “manufacturing industry”.

Apart from the fact that US, European Union, and China have different positions on the creation of a data ownership right,¹⁹⁶⁹ all have recognized that circulation and sharing of personal data is of great importance for data usage and ultimately for the digital economy. To this end, they have all introduced a wide variety of sub strategies as shown above. However, they have different approaches on how to achieve this in detail.

Ultimately, China’s goal is a “state-led data market, which would boost the digital economy by reducing transaction costs and allowing a smoother circulation of data”¹⁹⁷⁰. This is matched by case law from China, where the government “has recently launched a massive crackdown on them [companies]”¹⁹⁷¹, for example, through major antitrust cases based on competition policy, in response to the strong market power of some companies - for example, fining Alibaba a record USD 2.8 billion after an antitrust investigation.¹⁹⁷² This goes so far that the Chinese People’s Political Consultative Conference “suggested the creation of a national data bank from which users could purchase data sets; the income incurred would be distributed among all stakeholders according to their participation in generating, collecting, maintaining and exploiting the data”¹⁹⁷³.

As a result of this Section III.1.5 of Chapter IX, the following maturity levels can be identified:

Framework	GSMA classification	de Terwangne classification
US	Without ADPPA: Progressing With ADPPA: Advanced	Piecemeal/patchwork-model and sector-orientated model
Europe	Advanced	Comprehensive
APAC	Progressing China only: Advanced	Self-regulatory China only: Comprehensive
International organizations	Progressing	Self-regulatory

2. Data protection principles

One element of an at least “progressing” maturity is a data protection law as such. This should comprise certain “key components”. The question is what key components are. The UN stated in 2006 that

the overview of existing norms and rules suggests that although there are differences in approach, there is a commonality of interests in a number of core principles. The precedents and other relevant material, including treaties, national legislation, judicial decisions and non-binding instruments, point to the possibility of elaboration of a set of provisions that flesh out the issues relevant in data protection in light of contemporary

¹⁹⁶⁹ See Chapter VIII, Section II.

¹⁹⁷⁰ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 3.

¹⁹⁷¹ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 4.

¹⁹⁷² Zhong, R. [Raymond]. (1 September 2021). China fines Alibaba USD 2.8 Billion in Landmark Antitrust Case. *The New York Times*. <https://www.nytimes.com/2021/04/09/technology/china-alibaba-monopoly-fine.html>.

¹⁹⁷³ Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf. P. 4.

practice. Such an exercise would facilitate the preparation of a set of internationally acceptable best practices guidelines and would assist Governments in the development of national legislation. It would also assist the industry in devising models for self-regulation. The elaboration of a “third generation” of privacy principles would augur well with increasing calls for an international response on this matter. Although this is an area which is technical and specialized, it is also an area in which State practice is not yet extensive or fully developed.¹⁹⁷⁴

Key components are therefore considered to be, on the one hand, “data protection principles”, which are dealt with in this Section III.2; but also, on the other hand, “essential guarantees”, which are analyzed in Section III.3. This distinction is in many cases not clearly made by the frameworks in scope. The ASEAN Framework on Personal Data Protection, e.g., lists both under “principles”. The terminology of the GDPR will be used in Sections III.2 and III.3 of this Chapter. Since the GDPR is the most comprehensive regulation to date, as described above, other rulesets are to be placed in relation to the GDPR.

Convention 108+ lays down an obligation for the Member States to enact measures in their domestic law to give effect to the provisions of this Convention and secure their effective application, Art. 4(1) Convention 108+. Data shall be processed lawfully, fairly, and in a transparent manner (Arts. 5(3) and 5(4)(a) Convention 108+), processing shall be proportionate in relation to the legitimate purpose (Art. 5(1) Convention 108+), and be carried out based on the free, specific, informed and unambiguous consent (Art. 5(2) Convention 108+). Art. 5(4)(b) Convention 108+ sets out the principle of purpose limitation, Art. 5(4)(c) Convention 108+ the principle of data minimization, Art. 5(4)(d) Convention 108+ that of accuracy, Art. 5(4)(e) Convention 108+ provides for storage limitation, and Art. 7(1) Convention 108+ for integrity and confidentiality. Accountability is now an integral part of the protective scheme, with an obligation for the controllers to be able to demonstrate compliance with the data protection rules, Art. 10 Convention 108+. Art. 13 Convention 108+ clarifies that the Convention sets out only minimum standards, which does not prevent the Parties to provide greater protection in their national legal systems. The principles in Convention 108+ and the GDPR are therefore essentially equivalent:

Data protection principle	Convention 108+	GDPR
Lawfulness, fairness, and transparency	Arts. 5(3), 5(4)(a)	Art. 5(1)(a)
Purpose limitation	Art. 5(4)(b)	Art. 5(1)(b)
Data minimization	Art. 5(4)(c)	Art. 5(1)(c)
Accuracy	Art. 5(4)(d)	Art. 5(1)(d)
Storage limitation	Art. 5(4)(e)	Art. 5(1)(e)
Integrity and confidentiality	Art. 7(1)	Art. 5(1)(f)
Accountability	Art. 10(1)	Art. 5(2)

The ASEAN Framework on Personal Data Protection is based on the principles of lawfulness, fairness, and transparency, purpose limitation, accuracy, data security, storage limitation, and accountability. Data minimization is not mentioned. The APEC Privacy Framework 2015 regulates similar principles, though storage limitation is not included. Nevertheless, these APEC rules are stronger since they include the data minimization principle and have a more comprehensive and clearer wording than ASEAN. The ASEAN rules state in para. 12 that “there should be flexibility in implementing these principles”. For example, the purpose limitation principle could be

¹⁹⁷⁴ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Para. 12.

read into para. 6(b) ASEAN Framework on Personal Data Protection, but the wording “[purposes] that a reasonable person would consider appropriate in the circumstances” does not seem to clearly prohibit a change of purpose. Moreover, although these ASEAN rules mention the principle of lawfulness, it refers firstly only to consent (the conditions of which are not further explained), and, secondly, vaguely to “authorized or required under domestic laws and regulations”.

The UN encompasses States worldwide, but it has not yet fulfilled the role of a global data protection standard. Rather, its Guidelines are general, non-binding data protection principles. The UN has potential for finding a compromise between States, but the current Guidelines would have to be revised. In contrast to the OECD Guidelines 2013 and Convention 108+, the likelihood of a revised UN Guideline is low. Significantly, the International Data Protection Conference, in its 2007 declaration, temporarily moved away from the UN’s ability to create global data protection standards as an international organization and saw the International Organization for Standardization as a regulatory tool. The UN “International Law Commission” (ILC) decided in 2006 to include the issue of transborder data movements in its long-term work program.¹⁹⁷⁵ The proposal was based on the assumption that there is an “emerging trend” towards an international concept of data protection. This concept was based on general principles in data protection, on which despite the divergent national approaches there is agreement. This commission identified that international binding and non-binding instruments, as well as the national legislation adopted by States, and judicial decisions reveal a number of core principles, including: (a) lawful and fair data collection and processing; (b) accuracy; (c) purpose specification and limitation; (d) proportionality; (e) transparency; (f) individual participation and in particular the right to access; (g) non-discrimination; (h) responsibility; (i) independent supervision and legal sanction; (j) data equivalency in the case of TFPD; and (k) the principle of derogability.¹⁹⁷⁶ Paras. 1 and 5 of the UN Guidelines regulate only the “principle of lawfulness, fairness and transparency”. Accordingly, personal data may not be processed in unfair or unlawful manner. They may not be used for purposes which are contrary to purposes and principles of the UN Charter. The principles of purpose limitation, accuracy, and data security are included in paras. 2, 3, and 7 of the UN Guidelines, while accountability, storage limitation and data minimization are not mentioned.

Similar principles also appeared in a study by the OECD.¹⁹⁷⁷ In 1978, the OECD Expert Group on Drafting Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data had already discussed whether the OECD Guidelines should be formulated in general or for each specific areas and ultimately opted for general regulations.¹⁹⁷⁸ After this was determined, difficulties were caused to this expert group to select the principles of data protection and to decide how detailed these should be defined. The OECD Guidelines 2013 include all principles of the GDPR, except data minimization and storage limitation. The only significant positive addition in the OECD Guidelines 2013 compared to the OECD Guidelines 1980 is a new part on “implementing accountability” (para. 15), which introduces additional obligations on data controllers, including breach notification requirements.

¹⁹⁷⁵ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. P. 217 ff.

¹⁹⁷⁶ UN. (2013). *Yearbook of the International Law Commission 2006*. United Nations publications. A/CN.4/SER.A/2006/Add.1 (Part 2). Annex IV. Paras. 11, 23.

¹⁹⁷⁷ UNCTAD. *Data protection regulations and international data flows: Implications for trade and development*, UNCTAD/WEB/DTL/STICT/2016/1/iPub, (2016). P. 57.

¹⁹⁷⁸ OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum*,

<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#preface>. Para. 19.

For the US framework, at State level, common sense seems to exist only for three principles: Opt-in consent, Data minimization, nondiscrimination, and no data-use discrimination.¹⁹⁷⁹ At US federal level, ADPPA would encompass all principles known to the GDPR.

For China, PIPL guarantees the same principles as the GDPR. WTO rules do not contain neither data protection principles nor essential guarantees. As a result of Chapter IX Section III.2, the following data protection principles can be identified:

¹⁹⁷⁹ Klosowski, T. [Thorin]. (6 September 2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *The New York Times*. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us>.

Data Protection Principles	US	Europe	China	APEC	ASEAN	UN	OECD
Lawfulness, fairness, and transparency	Sec. 201, 202 ADPPA	Arts. 5(1a), 6 GDPR	Arts. 5, 7 PIPL	Paras. 13, 15, 18 Privacy Framework 2015	Paras. 6(a), 6(i) Framework on Personal Data Protection	Paras. 1, 5 UN Guidelines	Paras. 7, 8, 12 OECD Guidelines 2013
Purpose limitation	Sec. 101 ADPPA	Art. 5(1b) GDPR	Art. 6 PIPL	Para. 19 Privacy Framework 2015	Para. 6(b) Framework on Personal Data Protection	Para. 3 UN Guidelines	Paras. 9, 10 OECD Guidelines 2013
Data minimization	Sec. 101 ADPPA	Art. 5(1c) GDPR	Arts. 6, 19 PIPL	Para. 18 Privacy Framework 2015			
Accuracy	Sec. 301 ADPPA	Art. 5(1d) GDPR	Art. 8 PIPL	Para. 21 Privacy Framework 2015	Para. 6(c) Framework on Personal Data Protection	Para. 2 UN Guidelines	Para. 8 OECD Guidelines 2013
Storage limitation	Sec. 208 ADPPA	Art. 5(1e) GDPR	Art. 19 PIPL		Para. 6(g) Framework on Personal Data Protection		
Integrity and confidentiality	Sec. 208 ADPPA	Art. 5(1f) GDPR	Art. 9 PIPL	Para. 22 Privacy Framework 2015	Para. 6(d) Framework on Personal Data Protection	Para. 7 UN Guidelines	Para. 11 OECD Guidelines 2013
Accountability	Sec. 301-304 ADPPA	Art. 5(2) GDPR	Arts. 9, 49ff. PIPL	Para. 26 Privacy Framework 2015	Para. 6(h) Framework on Personal Data Protection		Paras. 14, 15, 16 OECD Guidelines 2013

Different approaches stand out within the prerequisites for a lawful processing of personal data and accountability. Three (sub)principles should therefore be mentioned separately because of their special position in this comparison of laws.

Except for the UN Guidelines, all regimes explicitly include consent as a legal basis for processing personal data. ADPPA, APEC, ASEAN, OECD Guidelines 2013, and PIPL focus on this ground of justification. ADPPA would set the same requirements to consent as the GDPR. However, OECD, APEC, and ASEAN have a broader interpretation; these three “require that, where appropriate, individuals should be provided with clear,

prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information”¹⁹⁸⁰. The GDPR is more stringent through its interpretation of consent as “freely given, specific, informed and unambiguous” and “explicit consent”. Notably absent from PIPL is a legal basis comparable to “legitimate interests” under the GDPR. Without that basis, consent is likely to remain a more central requirement under the PIPL than under the GDPR.

The principle of non-discrimination can also be seen as part of the “fairness” principle, according to which sensitive data that could be used for discrimination purposes, such as ethnic origin, sexual orientation, political or religious beliefs, or trade union membership, may not be processed. It is governed by para. 5 UN Guidelines, para. 19(i) OECD Guidelines 2013, para. 33 APEC Privacy Framework 2015, Sec. 207 ADPPA and Recital 75 GDPR. The regulations in China and ASEAN do not contain this subprinciple.

Except for the UN Guidelines, all frameworks include the principle of accountability, but the compliance requirements and execution differ. In ADPPA, all legal entities in scope of this proposed Act must designate one or more data security officers responsible for complying with the law. “Large data holders” (like the European definition of VLOPs) must also have a data protection officer responsible and complete a biennial privacy impact assessment. Large data holders “that use algorithms” must also submit annual algorithmic impact assessments to the FTC detailing steps they are taking to mitigate potential harm from their algorithms. In APEC, compliance assessments are done by the AA of each Member State. Under the GDPR, controllers and processors are expected to put into place comprehensive but proportionate governance measures to this end. ASEAN maintains accountability as a principle but has yet to develop an implementation process around accountability.

3. Essential guarantees

Following *Schrems I*, which included clarifications by the CJEU on Arts. 7, 8, 47 and 52 of the Charter, and the jurisprudence of the ECtHR related to Art. 8 ECHR, essential guarantees were identified first by the WP29. The EDPB further developed those guarantees based on the *Schrems II*.¹⁹⁸¹ The EDPB considered in its Recommendations 02/2020 that the legal requirements to make limitations to the data protection rights justifiable can be summarized in four essential guarantees:

- Guarantee A: The processing described therein must be based on clear, precise and accessible legal rules;
- Guarantee B: The processing carried out for the pursuit of legitimate purposes must be necessary and proportionate;
- Guarantee C: An independent monitoring mechanism must be in place;
- Guarantee D: There must be effective legal remedies for data subjects.¹⁹⁸²

¹⁹⁸⁰ GSMA. (September 2018). *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC can Protect Data and Drive Innovation*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf. P. 19.

¹⁹⁸¹ See in detail in Chapter II, Section II.3.4.4.c.

¹⁹⁸² EDPB. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, (10 November 2020),

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf. Para. 24.

Although a classification of a country under the GSMA or the de Terwangne criteria¹⁹⁸³ can be informative for appropriateness, it does not necessarily have to be. Rather, the decisive factor is whether a State can respect the essential guarantees “to make sure interferences with the rights to privacy and the protection of personal data, through surveillance measures, when transferring personal data, do not go beyond what is necessary and proportionate in a democratic society”¹⁹⁸⁴. From the perspective of the European framework, this is required not only by the GDPR, but also by Convention 108+.

The assessment as to whether the level of protection is appropriate must take into account the principles of the Convention, the extent to which they are met in the recipient State or organization – in so far as they are relevant for the specific case of transfer – and how the data subject is able to defend his or her interests where there is non-compliance. The enforceability of data subjects’ rights and the provision of effective administrative and judicial redress for the data subjects whose personal data are being transferred should be taken into consideration in the assessment. Similarly, the assessment can be made for a whole State or organization thereby permitting all data transfers to such a destination.¹⁹⁸⁵

The guarantees set out by Convention 108+ are essentially equivalent to those of the GDPR, the ECHR, and the Charter, which results in a consistency of the European rules:

¹⁹⁸³ See Chapter IX, Section III.1.5.

¹⁹⁸⁴ EDPB. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, (10 November 2020),

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf. Para. 1.

¹⁹⁸⁵ Explanatory Report to Convention 108+. Para. 112.

Essential guarantees	Convention 108+	Charter (+CJEU interpretations)	ECHR Art. 8 (+ECtHR interpretations)	GDPR Art. 46 (2) (c) (+EDPB Recommendation 02/2020)
Processing should be based on clear, precise, and accessible rules	Preamble („rule of law”), Art. 8	Arts. 8(2), 52(1); <i>Schrems II</i> , para. 173, 175, 180; <i>Privacy International</i> , para. 65, 68	<i>S. u. Marper v. UK</i> , 30562/04, para. 95ff.; <i>Liberty and others v. UK</i> , 58243/00, para. 63	P. 8
Necessity and proportionality regarding the legitimate objectives pursued need to be demonstrated	Art. 5(1)	Art. 52(1); <i>Schrems II</i> , para. 174-176, 180; <i>La Quadrature du Net and others</i> , para. 131, 136, 137; <i>Privacy International</i> , para. 78	<i>S. u. Marper v. UK</i> , 30562/04, para. 67-69ff.	P. 8
An independent oversight mechanism should exist	Art. 15	<i>Schrems II</i> , para. 179; <i>La Quadrature du Net and others</i> , para. 168, 189	<i>Klass and others v. Germany</i> , 5029/71, para. 17, 51; <i>Zakharov v. Russia</i> , 47143/06, para. 258, 283 and 287-283; <i>Iordachi and Others v. Moldova</i> , 25198/02, para. 40, 51	P. 8
Effective remedies need to be available to the individual	Art. 9	Art. 47; <i>Schrems II</i> , para. 95, 194-197; <i>La Quadrature du Net and others</i> , para. 190-191	<i>X and Y v. Netherlands</i> , 8978/80, para. 27; <i>Zakharov v. Russia</i> , 47143/06, para. 234	P. 8

In this Section III.3 the question arises whether the US framework and the domestic law in China reach such an essentially equivalent level or not. For the US framework, considerations are significantly related to the EU-US arena and the (domestic) US arena.¹⁹⁸⁶

At the time of closing the research for this thesis, the EU-US arena has been influenced by the provisional agreement on the EU-US DPF. According to a White House statement¹⁹⁸⁷, the following measures to implement the objectives of the EU-US DPF would be taken. There should be a new set of rules and binding safeguards to limit US intelligence agencies' access to data to what is necessary and proportionate to protect national security. To this end, US intelligence agencies are to establish procedures to

¹⁹⁸⁶ See also Chapter IX, Section II.1.; and Chapter IX, Section II.2.

¹⁹⁸⁷ USA, The White House. *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework>, (25 March 2022).

ensure effective oversight of the new privacy and civil liberties standards. A new “multi-layer redress mechanism” for investigating and resolving complaints from Europeans about access to data by US intelligence agencies is to be introduced, including a “Data Protection Review Court”. There are to be obligations on companies processing data transferred from the EU, including the obligation to self-certify their compliance with the principles by the US Department of Commerce, and specific monitoring and review mechanisms will be put in place.

This provisional agreement between the stakeholders in the EU and the US is a first important step towards a new agreement after the annulment of the Privacy Shield. However, it is first and foremost a political decision and not a change to the existing legal framework in the US; the latter was the subject of investigation in *Schrems I* and *Schrems II*. Although these bilateral negotiations play at highest political stakeholder level, the two sides across the Atlantic have hardly converged on a substantial level since *Schrems II*. Based on the preamble of the Privacy Shield alone, it was apparent that the US and the EU both recognize that they share the goal of promoting “privacy”, but each takes a different legal approach. According to the EU’s intention, which follows from the adequacy decision on the Privacy Shield, data subjects should continue to benefit from the level of protection that the EU ensures. The US has merely stated the goal of strengthening trade internationally. A higher level of protection can therefore – at this point – not be explicitly assumed as a mutual intention of the EU and the US. This means that in a future agreement, a common understanding should be included in the preamble to allow for a teleological interpretation of the norm text, if necessary, to avoid future problems in determining measures to improve judicial redress.

One measure mentioned in the factsheet of the EU-US DPF is the establishment of a “Data Protection Review Court” and a “multi-layer redress mechanism”.¹⁹⁸⁸ Christakis/Propp/Swire addressed the question how this could meet the requirements set by the CJEU in *Schrems II* and proposed a three-step approach.

First, the U.S. Department of Justice should issue a binding regulation creating within that executive agency an independent “Foreign Intelligence Redress Authority” (FIRA). Second, the President should issue a separate Executive Order providing the necessary investigative powers and giving FIRA’s decisions binding effect across the intelligence agencies and other components of the U.S. government. Finally, European individuals could obtain judicial review of an independent redress decision by using the existing Administrative Procedure Act.¹⁹⁸⁹

The first two steps seem to be covered by the announcement¹⁹⁹⁰ of an EO. However, the effects in practice of these remain to be seen, whether this EO would protect the officials appointed to this court against dismissal or revocation,¹⁹⁹¹ whether the court would be protected against external intervention or pressure liable to jeopardize the independent judgment of its members as regards proceedings before them,¹⁹⁹² whether it would

¹⁹⁸⁸ USA, The White House. *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework>, (25 March 2022).

¹⁹⁸⁹ Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (16 February 2022). EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers. *European Law Blog*. <https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers>.

¹⁹⁹⁰ USA, The White House. *FACT SHEET: President Biden to Sign Executive Order Protecting Access to Reproductive Health Care Services*, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services>, (8 July 2022).

¹⁹⁹¹ Required in *Schrems II*. Para. 195

¹⁹⁹² Required in: *Schrems II*. Para. 213

ensure the principle of impartiality,¹⁹⁹³ and whether it would have enough knowledge and understanding of the activities of the IC to fulfill its role effectively, while at the same time having sufficient distance from the IC to be able to act independently.¹⁹⁹⁴ Christakis/Propp/Swire suggested rather succinctly that “the U.S. Government could commit in the EU/US adequacy arrangement to maintain this EO in force”¹⁹⁹⁵. It remains questionable how this commitment should be maintained in the future under US law. Also, in another article a month earlier, Christakis/Propp/Swire themselves noted that “a law can set limits on executive discretion that only may be changed by a subsequent statute” and is therefore “a stable, permanent and objective way”;¹⁹⁹⁶ this is what an EO does not seem to be able to achieve.

Concerning the third step proposed by Christakis/Propp/Swire, it is questionable whether such a non-judicial body (the FIRA) could suffice to meet the European framework’s requirements. As Politico reported, “officials and others briefed on discussions paint a picture where EU citizens will be able to directly (or, in a back-up option, via their national governments) submit complaints to an independent judicial body if they believe U.S. national security agencies have unlawfully handled their personal information. That redress mechanism, bizarrely, may go further than what is available to U.S. citizens when they want to complain about government data access”¹⁹⁹⁷. Christakis/Propp/Swire were also concerned that “since the FIRA approach has not been judicially tested, some legal uncertainty concerning standing to bring the APA [Administrative Procedure Act] suit in federal court would remain. FOIA practice provides a good legal basis for meeting the standing requirement through challenging agency action itself, but [the] *Transunion* [case]¹⁹⁹⁸ highlighted the level of privacy injuries [“concrete injury”] which must be shown to enable a decision in federal court”¹⁹⁹⁹ and hereby raised the needed level for a standing in US court. *Solove / Keats Citron* resumed therefore that *Transunion LLC v. Ramirez* severely limited the effective enforcement of data protection laws. They contended that “existing standing doctrine incorrectly requires concrete harm. Moreover, when assessing harm, the Court has a crabbed and inadequate understanding of privacy harms. Additionally, allowing courts to nullify private rights of action in federal privacy laws is a usurpation of legislative power that upends the compromises and balances that Congress establishes in laws. Private rights of action are essential enforcement mechanisms.”²⁰⁰⁰

The advantage of a non-statutory solution would be that no US Congressional approval would be required. Nevertheless, “it is increasingly unlikely that Congress will pass any

¹⁹⁹³ Required in: *Schrems II*. Para. 213

¹⁹⁹⁴ Required in: WP29. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, WP 238, (13 April 2016). P. 49.

¹⁹⁹⁵ Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (16 February 2022). EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers. *European Law Blog*. <https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers>.

¹⁹⁹⁶ Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (16 February 2022). EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers. *European Law Blog*. <https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers>.

¹⁹⁹⁷ Scott, M. [Mark]. (3 February 2022). Digital Bridge: Privacy Shield update 3.0 – Semiconductor subsidies – EU-US policy spat. *Politico*. <https://www.politico.eu/newsletter/digital-bridge/privacy-shield-update-3-0-semiconductor-subsidies-eu-us-policy-spat>.

¹⁹⁹⁸ USA. *Transunion LLC v. Ramirez*, Supreme Court, No. 20–297.

¹⁹⁹⁹ Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (16 February 2022). EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers. *European Law Blog*. <https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers>.

²⁰⁰⁰ Solove, D. [Daniel] and Keats Citron, D. [Danielle]. (2022). *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*. 101 Boston University Law Review Online 62 (2021), GWU Legal Studies Research Paper No. 2022-06, GWU Law School Public Law Research Paper No. 2022-06, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895191.

digital-focused bills before lawmakers shut down ahead of November's midterms"²⁰⁰¹. This could also be because "congress historically has been reluctant to regulate in great detail how the President conducts foreign policy and protects national security"²⁰⁰². Moreover, as Christakis/Propp/Swire also noted, it would be "hard to explain to Congress why [EU data subjects] should get greater rights than Americans. On the other hand, if redress rights were also to be conferred on U.S. data subjects, then a novel and complex set of institutional changes to the overall U.S. surveillance system would be needed. [...] It would be difficult for U.S. legislators to vote for a statute without knowing in advance whether the CJEU will accept it as good enough."²⁰⁰³

However, in the case of a non-statutory solution, the separation of powers could be jeopardized. Cohn rightly noted that "the exercise of unilateral, non-statutory executive powers in a democratic society directly challenges the basic democratic principles that justify exercise of force in the social and economic spheres. Two central values, representation, and deliberation are compromised."²⁰⁰⁴ Christakis/Propp/Swire also noted that "there is greater democratic legitimacy if the legislature passes a statute"²⁰⁰⁵. As also noted above²⁰⁰⁶, of relevance is in this respect into which of the categories elaborated in the *Steel Seizure* case the Biden Administration's executive powers would fall to enact an EO "that will form the basis of the Commission's assessment in its future adequacy decision"²⁰⁰⁷. The key criterion here is whether the US Congress authorized, did not address, or even prohibited such conduct by the POTUS in the first place. The separation of powers problem could exist, however, even if US Congress would seek a statutory solution, as the US Congressional Research Service noted.

Congress might adopt statutory requirements addressing the CJEU's concerns. For instance, it could amend FISA to prohibit bulk intelligence collections and require court approval with respect to each target of surveillance. It could further create a cause of action that would allow foreign subjects to bring complaints before a tribunal if they believe intelligence agencies have collected or used their data in an unlawful way. These solutions may raise complex constitutional issues, such as separation of powers and Article III standing concerns [...].²⁰⁰⁸

²⁰⁰¹ Scott, M. [Mark]. (13 January 2022). Digital Bridge: US lawmaking stalled – Europe's (other) digital rules – France's Cédric O". *Politico*. <https://www.politico.eu/newsletter/digital-bridge/us-lawmaking-stalled-europes-other-digital-rules-frances-cedric-o>.

²⁰⁰² Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (31 January 2022). EU/US Adequacy Negotiations and the Redress Challenge: EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an "Essentially Equivalent" Solution. *European Law Blog*. <https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution>.

²⁰⁰³ Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (31 January 2022). EU/US Adequacy Negotiations and the Redress Challenge: EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an "Essentially Equivalent" Solution. *European Law Blog*. <https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution>.

²⁰⁰⁴ Cohn, M. [Margit]. (2015). Non-Statutory Executive Powers in Five Regimes: Assessing Global Constitutionalism in Structural-Institutional Contexts. *The International and Comparative Law Quarterly*, Cambridge University Press, 64(1), 65–102. P. 101.

²⁰⁰⁵ Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (31 January 2022). EU/US Adequacy Negotiations and the Redress Challenge: EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an "Essentially Equivalent" Solution. *European Law Blog*. <https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution>.

²⁰⁰⁶ Chapter III, Section II.1.1.2.

²⁰⁰⁷ USA, The White House. *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework>, (25 March 2022).

²⁰⁰⁸ USA, Congressional Research Service. *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, R46724, <https://crsreports.congress.gov/product/pdf/R/R46724>, (17 March 2021). P. 13.

These concerns regarding “standing” have been exacerbated by the *Fazaga* case²⁰⁰⁹, in which the US Supreme Court upheld the state secrecy principle for FISA. In addition, the objectives of the EU-US DPF may contradict interpretations by the US judiciary that all non-US persons have no Fourth Amendment rights.²⁰¹⁰

It could also be conceivable to provide the FTC with greater authority to bring data protection enforcement actions and remove limitations on the FTC’s jurisdiction with respect to common carriers and nonprofit organizations.²⁰¹¹ Since – except for the CPRA – no US State law yet guarantees a private right of action, there are nevertheless opinions to compensate this lack with increased resources for the FTC. Ashkan Soltani, former chief technologist at the FTC, argued that “enforcement is a really important facet. If there’s adequate enforcement – legal protections and regulatory resources – I don’t think it’s a dealbreaker to forgo a private right to action”²⁰¹². Hayley Tsukayama from the EFF said that “especially in those states where they don’t allow a private right [of action], to then also underfund the public enforcement – it’s just an insult to injury”.²⁰¹³ On 28 May 2021, POTUS Joe Biden proposed a budget which would give an 11% funding increase to the FTC of USD 389.8 million and would increase its staff to about 1,250 in the 2022 fiscal year.²⁰¹⁴ The House Committee on Energy and Commerce voted in favor of an unprecedented USD 1 billion over 10 years to the FTC to establish and operate a new privacy bureau, an initiative that is supported by the ACLU and 26 other civil rights and advocacy groups.²⁰¹⁵ For the year of 2022, therefore “odds are likely that the FTC will seek to optimize and strengthen its authority via its new left-leaning leadership”, which highlights “future FTC strategies seeking stronger privacy enforcement authority”.²⁰¹⁶ This strategy was also confirmed²⁰¹⁷ by the new FTC chairwoman, Lina Khan, and in a blog in July 2022, the FTC commented that it “does not tolerate companies that over-collect, indefinitely retain, or misuse consumer data” and is “committed to fully enforcing the law against illegal use and sharing of highly sensitive data” such as location- and health-related information.²⁰¹⁸ This call comes “close on the heels of President Joe Biden’s executive order calling on the commission to consider taking steps to protect consumers” privacy when seeking information about and provision of reproductive health care services.²⁰¹⁹ The US States of Virginia and California had

²⁰⁰⁹ See Chapter III, Section II.1.2.4.

²⁰¹⁰ “It is long settled as a matter of American constitutional law that foreign citizens outside U. S. territory do not possess rights under the U. S. Constitution. Plaintiffs do not dispute that fundamental principle.” USA. *US Agency for Int’l Dev. v. Alliance for Open Soc’y Int’l, Inc.*, Supreme Court, 140 S. Ct. 2082, 2086 (2020)

²⁰¹¹ USA, Congressional Research Service. *U.S.-EU Privacy Shield and Transatlantic Data Flows*, R46917, (22 September 2021). P. 23.

²⁰¹² Klosowski, T. [Thorin]. (6 September 2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *The New York Times*. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us>.

²⁰¹³ Klosowski, T. [Thorin]. (6 September 2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *The New York Times*. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us>.

²⁰¹⁴ Bartz, D. [Diane]. (28 May 2021). *Biden seeks 11% jump in FTC funding as Big Tech cases loom*. Reuters. <https://www.reuters.com/technology/biden-seeks-11-jump-ftc-funding-big-tech-cases-loom-2021-05-28>.

²⁰¹⁵ Reuters. (15 September 2021). U.S. panel votes to approve USD 1 billion for FTC privacy probes. <https://www.reuters.com/business/us-panel-votes-approve-1-billion-ftc-privacy-probes-2021-09-14>. // Reuters. (23 September 2021). ACLU, 26 other groups support USD 1 billion boost for FTC privacy work. <https://www.reuters.com/world/us/aclu-26-other-groups-support-1-billion-boost-ftc-privacy-work-2021-09-23>.

²⁰¹⁶ Salvino, M. A. [Mary Ashley]. (1 November 2021). *Analysis: How Will the FTC Get Its Privacy Mojo Back*. <https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-how-will-the-ftc-get-its-privacy-mojo-back-in-2022>.

²⁰¹⁷ USA, Federal Trade Commission. *Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security*, Commission File No. P065401, https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf, (1 October 2021).

²⁰¹⁸ USA, Federal Trade Commission. *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use?utm_source=govdelivery, (11 July 2022).

²⁰¹⁹ USA, Federal Trade Commission. *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use?utm_source=govdelivery, (11 July 2022).

also increased their budgets.²⁰²⁰ It remains to be seen whether or not these financial aids will lead federal and State SAs to convergence with characteristics of SAs according to a European framework pattern.

Others preferred to “to create an entirely new regulatory agency that could police privacy issues and potentially even online competition, as proposed by prominent Democrats such as Sen. Kirsten Gillibrand (D-N.Y.), privacy advocates and former regulators”²⁰²¹; however, even these initiators stated that such new agency is “short of an independent agency”²⁰²², which would then again contrast with the European approach.

Since Directive 95/46, it is still questionable whether US companies could lose their incentive to join a framework such as the EU-US DPF because European data protection law might be already directly applicable to them.²⁰²³ Colonna stated in this respect that “in such cases the major benefits of joining the program – the ability to rely on industry dispute resolution mechanisms, US law to interpret the principles, and US courts and administrative bodies to hear claims – will be removed”²⁰²⁴. Although Colonna stated this with regard to Art. 4 Directive 95/46, her considerations also apply to Art. 3 GDPR. Art. 3 GDPR could therefore have the potential to compromise the EU-US DPF in this respect.

It is also noticeable that both sides of the Atlantic speak of “democratic society”. This expression can also be found in Art. 8(2) ECHR, Art. 13(3) LED, Art. 14(4)(c) Convention 108+²⁰²⁵, Arts. 6 and 23(1) GDPR, Art. 29(2) UDHR, in the context of the proportionality test of Art. 17 ICCPR, the EDPB Recommendations 02/2020²⁰²⁶, the Guide to the Case Law of the ECtHR, the CJEU case law (*Schrems II*), and Section 26 of UK’s Data Protection Act 2018. This suggests that Western democracies want to differentiate themselves from other countries that are not “democratic societies” but have nonetheless raised the level of data protection. Such countries include China in particular. The EU and the US nevertheless recognized that

while we are still the most influential regulators, both the EU and the US face increasing standard competition from third country stakeholders. Where both sides agree, the world usually follows. This is why we must reactivate proposals for EU-US standards cooperation and re-engage on conformity assessment negotiations. Where possible, the EU and the US should systematically align positions within international standard setting bodies.²⁰²⁷

This seems to be a contradiction and a more precise definition of the term “democratic society” will therefore become more and more important, especially for the EU-US arena.

²⁰²⁰ The California CPPA will receive USD 10 million in annual funding. The Virginia state attorney general’s office handles enforcement with USD 400,000 in funding, supplemented with fines and penalties.

²⁰²¹ Lima, C. [Cristiano]. (16 September 2021). Why Democrats are rallying around creating a new FTC privacy bureau to police Big Tech. *The Washington Post*. <https://www.washingtonpost.com/politics/2021/09/16/why-democrats-are-rallying-around-creating-new-ftc-privacy-bureau-police-big-tech>.

²⁰²² Lima, C. [Cristiano]. (16 September 2021). Why Democrats are rallying around creating a new FTC privacy bureau to police Big Tech. *The Washington Post*. <https://www.washingtonpost.com/politics/2021/09/16/why-democrats-are-rallying-around-creating-new-ftc-privacy-bureau-police-big-tech>.

²⁰²³ See also above Chapter II, Section II.3.4.2.

²⁰²⁴ Colonna, L. [Liane]. (2014). Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?. *International Data Privacy Law*, 4(3), 203–221. P. 221.

²⁰²⁵ Explanatory Report to Convention 108+. Para. 108.

²⁰²⁶ EDPB. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, (10 November 2020),

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf. Para. 1.: “to make sure interferences with the rights to privacy and the protection of personal data, through surveillance measures, when transferring personal data, do not go beyond what is necessary and proportionate in a democratic society.”

²⁰²⁷ European Commission. *A new EU-US agenda for global change*, JOIN(2020) 22 final, (2 December 2020). P. 7.

The CoE Statute at least provides a definition that speaks of “individual freedom, political liberty and the rule of law, principles which form the basis of all genuine democracy”²⁰²⁸.

As Spies also explained, the problems that have arisen in the EU-US arena, not least as a result of *Schrems II*, can effectively only be solved by the political stakeholders.²⁰²⁹ Spies believes that the Biden administration could make achievements in Brussels with concrete commitments, namely with an EO, as also proposed by the “Open Technology Institute” (OTI). The latter noted that “in order for the U.S. government to create an effective and sustainable solution, it must institute reforms to the U.S. surveillance ecosystem”²⁰³⁰. These reforms, according to the OTI, would then improve rights for non-US persons as well as US persons, and would accordingly impact the evolution of US federal legislation. These measures – per the EO – would be easier to enact than a currently “utopian” change in US laws.²⁰³¹ The question is whether aligning US laws with the level of protection required by the CJEU is in fact so “utopian.” Although polls²⁰³² showed that more than half of US voters support a federal law on data protection, no such law yet exists. Because the EU-US DPF is “not yet so concrete that it makes any difference to organizations that transfer personal data to the US”, companies that wish to transfer personal data to the US “must therefore continue to establish a possible transfer basis [...] because there is no new transfer basis and adequacy assessment yet”.²⁰³³ Therefore, the following considerations remain also important in the context of a TIA required by the European SDPC to assess the level of protection in a recipient country.

The political situation in the US until end-2020 made it unlikely that a federal bill would be adopted by the US Senate at the 116th Congress. Now, after Joe Biden’s election as POTUS and Democrats control of the House, there is potential for the 117th Congress to enact federal legislation.²⁰³⁴ Should the proposed Data Accountability and Transparency Act 2020 be considered, a general prohibition of data processing, together with some exceptions, would mean a strong shift in the US towards the principle of prohibition of the GDPR. Should the proposed Safe Data Act or – even more – ADPPA become US law in this form, the US could eventually be completely given a European-style data protection law.

Before coming to the contents of ADPPA in comparison to the essential guarantees, one issue surrounding a potential federal data protection bill in the US must be addressed, which is the so-called “preemption doctrine”. Preemption is based on the supremacy clause of the Constitution,²⁰³⁵ according to which federal law supersedes conflicting State laws. It is therefore in question, if the US Congress would write “one national standard” that preempts effective State laws which currently offer a higher standard of data

²⁰²⁸ CoE. *Statute of the Council of Europe*, ETS No. 001, (5 May 1949). Preamble.

²⁰²⁹ Spies, A. [Axel]. (2021). EU-US-Privacy-Shield – eine schwierige Reparatur. *Zeitschrift für Datenschutz*, 2021(9). 478–481. P. 481.

²⁰³⁰ Bradford Franklin, S. [Sharon] and Sarkesian, L. [Lauren]. (7 April 2021). Strengthening Surveillance Safeguards After Schrems II. *New America*. <https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii>. P. 7.

²⁰³¹ Spies, A. [Axel]. (2021). EU-US-Privacy-Shield – eine schwierige Reparatur. *Zeitschrift für Datenschutz*, 2021(9). 478–481. P. 481.

²⁰³² “National data privacy legislation has consistently ranked as an important congressional agenda item for the public, with 79 percent of adults saying in 2019 that lawmakers should prioritize the effort and 83 percent showing support last year [2021] as state governments looked to do it themselves.” Teale, C. [Chris]. (12 January 2022). *More Than Half of Voters Back a National Data Privacy Law*. <https://morningconsult.com/2022/01/12/federal-data-privacy-legislation-polling>.

²⁰³³ Datatilsynet. Ny aftale om udveksling af personoplysninger mellem EU og USA, <https://www.datatilsynet.dk/internationalt/internationalt-nyt/2022/mar/ny-aftale-om-udveksling-af-personoplysninger-mellem-eu-og-usa>, (29 March 2022).

²⁰³⁴ IAPP. (29 April 2021). *Keynote: EU-U.S. Data Transfers: The Road Ahead*.

<https://www.linkedin.com/video/live/urn:li:ugcPost:6793534522072801280/?isInternal=true>

²⁰³⁵ US Constitution, Art. 6(2).

protections, such as CCPA/CPRA. The Supreme Court identified two ways in which federal law can preempt State law. “First, federal law can expressly preempt state law when a federal statute or regulation contains explicit preemptive language. Second, federal law can impliedly preempt state law when its structure and purpose implicitly reflect Congress’s preemptive intent”.²⁰³⁶ A federal law could enact a so-called “field preemption” which would supersede all State laws related to certain activities of certain legal entities to be covered. Depending on the scope of this “field”, such a federal law could sweep away a body of State law developed over decades. As described above²⁰³⁷, three US States have regulated a comprehensive field of data protection, while other States did so with smaller fields but sometimes more intensively than those of the comprehensive approach. In any case, a preemption by federal law could affect a range of predominantly local interests. It is understandable that these interests are more strongly defended as soon as a State law already guarantees a higher level of protection. The CPRA is considered as such a stronger law.²⁰³⁸ Bloomberg therefore reported that “California Democrats want to make sure the federal standard doesn’t weaken their state law by taking precedent over it. The California Privacy Protection Agency sent Speaker Nancy Pelosi (D-Calif.) a memo outlining why the bipartisan bill [ADPPA] would harm residents in her home state. [...] While extending privacy protections nationwide is important, under this bill, it would come at the expense of Californians’ rights”.²⁰³⁹ That is why it was also tried “to exempt the California Consumer Privacy Act and the California Privacy Rights Act from the bill’s preemption provisions [which] was not taken up following a 48-8 roll call vote”²⁰⁴⁰. In contrast, “opponents of broad preemption often appeal to the importance of policy experimentation, the greater democratic accountability that they believe accompanies state and local regulation, and the gap-filling role of state common law in deterring harmful conduct and compensating injured plaintiffs”²⁰⁴¹. “In the modern privacy realm, many privacy advocates [...] resist any prospect of closing off state legislative action”²⁰⁴². Proponents of broad federal preemption on the other hand see “the benefits of uniform national regulations and the concentration of expertise in federal agencies”²⁰⁴³. For the area of data protection law, this could mean that “the single most important reason for industry to accept and support federal privacy legislation is an understandable desire for a single national set of rules to follow”²⁰⁴⁴. Since the field of data protection does not stop neither at State borders, nor at federal borders, “industry leaders want to avoid differing – and potentially conflicting – state laws that would set privacy rules based on a user’s residence or current location”²⁰⁴⁵. It would also be possible, as Kerry / Morris suggested, to only “preempt inconsistent laws rather than only those that are directly conflicting, and to omit the exception permitting state laws with a greater level of privacy protection than the federal law”²⁰⁴⁶. The question of preemption has not been addressed in the Safe Data Act. ADPPA would supersede many existing

²⁰³⁶ USA, Congressional Research Service. *Federal Preemption: A Legal Primer*, R45825, (23 July 2019). P. 2.

²⁰³⁷ Chapter III, Section II.2.

²⁰³⁸ CPPA Executive Director Ashkan Soltani said that “while I appreciate suggestions by advocates and others about how the ADPPA may be stronger than California law, I assure you that in my and the staff’s expert opinion that it is not.” Duball, J. [Joseph]. (29 July 2022). *Calif. privacy agency takes aim at dismantling federal privacy preemption*. <https://iapp.org/news/a/cppa-takes-aim-at-dismantling-american-data-privacy-and-protection-acts-preemption>.

²⁰³⁹ Curi, M. [Maria]. (13 July 2022). *California Democrats Demand Stronger Privacy Protection Bill (2)*. *Bloomberg*. <https://news.bloomberglaw.com/privacy-and-data-security/california-democrats-push-for-stronger-privacy-protection-bill>.

²⁰⁴⁰ Duball, J. [Joseph]. (21 July 2022). *American Data Privacy and Protection Act heads for US House floor*. <https://iapp.org/news/a/american-data-privacy-and-protection-act-heads-for-us-house-floor>.

²⁰⁴¹ USA, Congressional Research Service. *Federal Preemption: A Legal Primer*, R45825, (23 July 2019). P. 1–2.

²⁰⁴² Kerry, C. F. [Cameron F.] and Morris, J. [John]. (19 June 2020). *Preemption: A balanced national approach to protecting all Americans’ privacy*. <https://www.brookings.edu/blog/techtank/2020/06/29/preemption-a-balanced-national-approach-to-protecting-all-americans-privacy>.

²⁰⁴³ USA, Congressional Research Service. *Federal Preemption: A Legal Primer*, R45825, (23 July 2019). P. 1.

²⁰⁴⁴ USA, Congressional Research Service. *Federal Preemption: A Legal Primer*, R45825, (23 July 2019). P. 1.

²⁰⁴⁵ USA, Congressional Research Service. *Federal Preemption: A Legal Primer*, R45825, (23 July 2019). P. 1.

²⁰⁴⁶ Kerry, C. F. [Cameron F.] and Morris, J. [John]. (19 June 2020). *Preemption: A balanced national approach to protecting all Americans’ privacy*. <https://www.brookings.edu/blog/techtank/2020/06/29/preemption-a-balanced-national-approach-to-protecting-all-americans-privacy>.

State data protection laws. However, it would exclude from preemption a long list of fields such as specific statutes on civil rights, criminal codes, student and employee privacy, data breach notification requirements, facial recognition, and financial and health records, including parts of the CPRA. This could fundamentally undermine the purpose of preemption, which in the context of the EU-US arena would be the achievement of a uniform level of data protection in the US.

GDPR, ADPPA, and PIPL, as examined above²⁰⁴⁷, cover the first two of the four essential guarantees. It remains to be examined which frameworks in scope of this thesis guarantee an “independent oversight mechanism” and “effective remedies to the individual”.

Effective remedies to the individual are initially dependent on the guarantee of certain data subject rights. The question is which of the data subjects are considered “essential”. The CJEU explained in *Schrems I* that

legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article.²⁰⁴⁸

The right to erasure and the right to correct are therefore deemed essential. In its decision *La Quadrature du Net*, the CJEU considered that notification is necessary “to enable the persons affected to exercise their rights under Articles 7 and 8 of the Charter to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased, as well as to avail themselves, in accordance with the first paragraph of Article 47 of the Charter, of an effective remedy before a tribunal”²⁰⁴⁹. The ECtHR has confirmed this view on the right to be informed in its *Zakharov* decision.²⁰⁵⁰ These judgments therefore added the rights to be informed and the right to access being essential. Besides the ASEAN Framework on Personal Data Protection and the WTO, all frameworks, and also the domestic law in China, include those four essential data subject rights as possible remedies.

For the other data subject rights, it can be concluded from the above that only PIPL includes all such rights known to the European framework. For the US framework, this needs to be considered in more detail. At US State level – until the proposed ADPPA – there seemed to be common sense only for these data subject rights: The right to access, the right to erasure, the right to data portability, the right to restrict data processing.²⁰⁵¹ In ADPPA, the right to restrict data processing is not explicitly mentioned, but the fact that individuals may opt out of the transfer (Sec. 204) seems to include this right. ADPPA also follows a risk approach through a “privacy impact assessment” which considers the benefits of its data practices against potential risks to individuals. As a special category of this risk approach, Sec. 207(c) ADPPA regulates a so-called “algorithm impact and evaluation”. ADPPA does not explicitly state that a data subject shall have the right not to be subjected to a decision based solely on automated processing, as provided for in

²⁰⁴⁷ Chapter IX, Section III.2.

²⁰⁴⁸ *Schrems I*. Para. 95

²⁰⁴⁹ *La Quadrature du Net* case. Para. 190.

²⁰⁵⁰ ECtHR, *Roman Zakharov v. Russia*, Judgment of 4 December 2015, Application no. 47143/06. Para. 234

²⁰⁵¹ Klosowski, T. [Thorin]. (6 September 2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *The New York Times*. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us>.

Art. 22 GDPR. However, Sec. 207(c) ADPPA requires the data subject to be informed and to be able to exercise his or her other rights under ADPPA. On the other hand, ADPPA grants the user the possibility to query his or her data and, if desired, to have it corrected or deleted by the data holder. ADPPA contains privileges for smaller organizations, such as not requiring data portability for smaller data holders and allowing them to delete, rather than correct, data. Children's privacy is particularly strictly protected. ADPPA also incorporates an approach similar to Privacy by Design. Although not a "principle" in the strict sense, this is still worth mentioning, because ADPPA goes even one step further than the GDPR; ADPPA regulates to establish a process for organizations to submit technical compliance programs for the agency's approval by outlining how they intend to meet or exceed the ADPPA's requirements. Large data holders must also have a privacy protection officer responsible. Most importantly when considering again the findings in *Schrems II*, ADPPA would provide a private right of action, which would allow individuals to bring civil actions seeking compensatory relief or injunctive relief against data holders. However, this right would not apply until two years after the law came into force. Citizens should have that right from day one, Cantwell urges:

For American consumers to have meaningful privacy protection, we need a strong federal law that is not riddled with enforcement loopholes. [...] Consumers deserve the ability to protect their rights on day one. [...] A series of notice requirements and coordination with states' attorneys general and the Federal Trade Commission would be required. It also would make private rights of action subject to a decision first by the state Attorney General and then the FTC.²⁰⁵²

The last sentence of this comment is not entirely correct, since individuals would first need to notify both their Attorney General and the FTC of their intent to sue, and those agencies would then decide whether to initiate proceedings. But there is a danger that if neither the FTC nor an Attorney General decides to pursue, the only lawsuits individuals would be proceeding with under the ADPPA are likely to be meritless.²⁰⁵³ In sum,

ADPPA provides for consumer data rights similar to the data subject rights in the GDPR. [...] However, in comparison to the data subject's rights under GDPR, the consumer data rights are subject to certain limitations. For example, back-up and archived data are excluded from the access right, the scope of access is restricted to the data processed within the last 24 months, and, depending on the size of the covered entity, the statutory response time is between 45 to 135 days (Sec. 203 ADPPA). Covered legal entities may rely on certain exceptions to refuse answering a request.²⁰⁵⁴

After an analysis of the various frameworks, the coverage of data subject rights can be determined as follows:

²⁰⁵² Curi, M. [Maria]. (3 June 2022). Bipartisan Draft Bill Would Fortify Children's Data Privacy (3). *Bloomberg*. <https://about.bgov.com/news/bipartisan-draft-bill-would-fortify-childrens-data-privacy-2>.

²⁰⁵³ Castro, D. [Daniel]. (6 June 2022). *Review of the Proposed "American Data Privacy and Protection Act, Part 1: State Preemption and Private Right of Action*. <https://itif.org/publications/2022/06/06/american-data-privacy-and-protection-act-review-part-1-state-preemption-and-private-right-of-action>.

²⁰⁵⁴ Osborne Clark. (8 August 2022). *ADPPA vs GDPR*. <https://www.osborneclarke.com/system/files/documents/22/08/10/ADPPA%20vs%20GDPR.pdf>. P. 6.

Data subject rights	US	Europe	China	APEC	ASEAN	UN	OECD
Right to be informed	Sec. 201, 202 ADPPA	Arts. 12-14 GDPR	Arts. 7, 17, 23, 30 PIPL	Paras. 23, 24, 25 APEC Privacy Framework 2015	Art. 6(i) Framework on Personal Data Protection	Para. 4 UN Guidelines 1990	Paras. 13(a), 13(b) OECD Guidelines 2013
Right to access	Sec. 203 ADPPA	Art. 15 GDPR	Arts. 44, 45 PIPL	Paras. 23, 24, 25 APEC Privacy Framework 2015	Art. 6(e)(i) Framework on Personal Data Protection	Para. 4 UN Guidelines 1990	Para. 13(a) OECD Guidelines 2013
Right to correct	Sec. 203 ADPPA	Art. 16 GDPR	Art. 46 PIPL	Paras. 23, 24, 25 APEC Privacy Framework 2015	Art. 6(e)(ii) Framework on Personal Data Protection	Para. 4 UN Guidelines 1990	Para. 13(d) OECD Guidelines 2013
Right to erasure	Sec. 203 ADPPA	Art. 17 GDPR	Art. 47 PIPL	Paras. 23, 24, 25 APEC Privacy Framework 2015		Para. 4 UN Guidelines 1990	Para. 13(d) OECD Guidelines 2013
Right to restrict processing		Art. 18 GDPR	Arts. 15, 44 PIPL	Para. 20 APEC Privacy Framework 2015			Para. 13(d) OECD Guidelines 2013
Right to data portability	Sec. 203 ADPPA	Art. 20 GDPR	Art. 45 PIPL				
Right to object	Sec. 204 ADPPA	Art. 21 GDPR	Arts. 15, 44 PIPL	Para. 20 APEC Privacy Framework 2015			Paras. 13(c), 13(d) OECD Guidelines 2013
Right in relation to automated decision making and profiling		Art. 22 GDPR	Arts. 24, 55 PIPL				

Remedies against interference with the right to data protection can be deemed “effective” – as the ECtHR noted – if they are “subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body”²⁰⁵⁵. The independent oversight over, in particular, the implementation of surveillance measures, was also taken into account by the CJEU in *Schrems II*.²⁰⁵⁶

Definitions on the requirement of “independent and impartial” differ slightly within the European framework. Art. 47 of the Charter guarantees such before a “tribunal” (understood as “judicial body”, as the official explanation suggests), while Art. 13 ECHR refers to a “national authority”, which does not necessarily need to be a judicial authority.²⁰⁵⁷ *Schrems II* found “the premise [...] that data subjects must have the possibility of bringing legal action before an independent and impartial court”²⁰⁵⁸, “the right to judicial protection”²⁰⁵⁹, “data subject rights actionable in the courts against the US authorities”²⁰⁶⁰, “the judicial protection of persons whose personal data is transferred to that third country”²⁰⁶¹, and “the existence of such a lacuna in judicial protection in respect of interferences with intelligence programs”²⁰⁶². The CJEU considered that an effective judicial protection against interferences can be ensured not only by a court, but also by a “body” which offers guarantees essentially equivalent to those required by Art. 47 of the Charter.²⁰⁶³ This indicates that some form of ultimate judicial review of an authority’s decision would be required.

Under PIPL, enforcement authorities responsible for the protection of personal data are the CAC, relevant departments of the State Council (such as the Ministry of Public Security, the State Administration for Market Regulation, the People’s Bank of China, and the National Health Commission), and relevant departments of county-level and higher local governments which perform such protection duties according to related regulations. PIPL therefore didn’t change the multi-centered supervision system in China, although PIPL in Arts. 60-65 now explains the various responsibilities in more detail. However, these are overlapping and too vague thanks to the repeated wording “other duties and responsibilities provided in laws or administrative regulations”. China does therefore probably not have an independent data protection authority like the EU Member States.

The CJEU annulled the Commission adequacy decision on the Privacy Shield Agreement because it determined that FISA Section 702 and EO 12333, even limited by PPD-28, are too permissive to meet standards of necessity and proportionality.²⁰⁶⁴ It is therefore questionable whether US surveillance statutes and procedures could sufficiently incorporate principles of “necessity and proportionality” required under Art. 52 of the Charter. After POTUS Biden signed the “Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities” on 7 October 2022, a closer look can be taken at its contents. Two major points of criticism stand out: proportional surveillance and the required remedy for data subjects. According to NOYB, this EO does not change the original problem of the proportionality of government access.²⁰⁶⁵ Mass surveillance would continue under the new EO, as all data sent to US providers

²⁰⁵⁵ ECtHR, *Klass et al v. Germany*, Judgment of 6 September 1978, Application no. 5029/71. Paras. 17, 51

²⁰⁵⁶ *Schrems II*. Paras. 179, 183

²⁰⁵⁷ ECtHR, *Klass et al v. Germany*, Judgment of 6 September 1978, Application no. 5029/71. Para. 67

²⁰⁵⁸ *Schrems II*. Para. 194

²⁰⁵⁹ *Schrems II*. Para. 194

²⁰⁶⁰ *Schrems II*. Para. 192

²⁰⁶¹ *Schrems II*. Para. 190

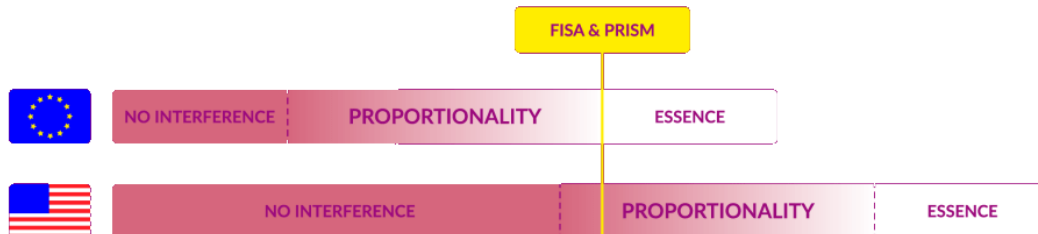
²⁰⁶² *Schrems II*. Para. 191

²⁰⁶³ *Schrems II*. Para. 197

²⁰⁶⁴ *Schrems II*. Para. 184

²⁰⁶⁵ NOYB. (7 October 2022). *New US Executive Order unlikely to satisfy EU Law*. <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>.

would still end up in programs such as PRISM or Upstream, Section 2(c)(ii) of this EO. This Section, they argued rightly, is an empty phrase that has been adopted without the same legal meaning. “If it would have the same meaning, the US would have to fundamentally limit its mass surveillance systems to comply with the EU understanding of proportionate surveillance.”²⁰⁶⁶



Source: NOYB, “Proportionality-graphic”²⁰⁶⁷

In this respect, the status quo would remain, which the CJEU has already twice considered in *Schrems I* and *Schrems II* to be unsatisfactory. This view is supported by an earlier report of the PCLOB with “recommendations, containing appropriate redactions to protect classified information, resulting from the Board’s review of one CIA counterterrorism activity conducted pursuant to E.O. 12333 (“Deep Dive 2”)”²⁰⁶⁸. The PCLOB found that the program lacked proper oversight. This report was a response to a letter from Sen. Ron Wyden and Sen. Martin Heinrich in which the senators asked for the PCLOB’s “Deep Dive II” report, which in part reviewed the CIA’s bulk collection program, be declassified. In the letter, the members of the Senate Intelligence Committee wrote that the CIA had “secretly conducted its own bulk program”, adding that the CIA’s collection program was “entirely outside the statutory framework that Congress and the public believe govern this collection, and without any of the judicial, congressional or even executive branch oversight that comes from [FISA] collection”²⁰⁶⁹. It therefore remains to be seen how the principles of “necessity and proportionality” would be implemented in practice, given the still strong position of the IC.

Moreover, the still existing interpretative differences in the European framework make it difficult to fully assess whether the proposed FIRA in the US could be subsumed under the interpretations of the ECtHR, Art. 47(2) Charter and Art. 6(1) ECHR. As an EO has the force of law, at least the criterion “established by law” would be fulfilled. ADPPA would create a new division within the FTC tasked with enforcing this law, and not a new authority, as demanded by some as described above. Therefore, the question remains unresolved how the FTC should be “independent”. It is also questionable whether the FTC would be granted the power to adopt decisions that are binding on the intelligence services, in accordance with legal safeguards on which data subjects could rely. NOYB argued that the “Data Protection Court” mentioned in the EO of 7 October 2022 is an executive body.²⁰⁷⁰ They argued further that the EO strongly resembles the former “ombudsman”, which was the point of contact for data subjects and was already declared inadequate by the CJEU. This means that a simple complaints body has now simply

²⁰⁶⁶ NOYB. (7 October 2022). *New US Executive Order unlikely to satisfy EU Law*. <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>.

²⁰⁶⁷ NOYB. (7 October 2022). *New US Executive Order unlikely to satisfy EU Law*. <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>.

²⁰⁶⁸ PCLOB. (10 February 2022). *Report and Recommendations on CIA Counterterrorism Activities Conducted Pursuant to E.O. 12333*. <https://www.pclob.gov/Oversight>.

²⁰⁶⁹ USA, Senate, *Letter of 13 April 2021*, https://www.wyden.senate.gov/imo/media/doc/HainesBurns_WydenHeinrich_13APR21%20-FINAL.pdf, (13 April 2021).

²⁰⁷⁰ NOYB. (7 October 2022). *New US Executive Order unlikely to satisfy EU Law*. <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>.

been renamed a court, in the hope that the requirements of Art. 47 Charter will be met. The procedure before the Data Protection Court also raises considerable doubts about effective legal protection since data subjects must go through a data protection authority and complaints are sent to a US official.

The EU-US DPF seems to indicate that the US might, despite the development around ADPPA, seek a non-statutory solution. The goal after that may be, as Christakis/Propp/Swire also indicated, that “if an adequate fix to the redress problem can be created at least in large part without new legislation, then it would be considerably easier for Congress subsequently to enact a targeted statute ratifying the new mechanism, perhaps adding other provisions to perfect an initial non-statutory approach.”²⁰⁷¹ This sounds comprehensible as US Congress still seems willing to consider

comprehensive national privacy legislation to protect U.S. personal data with data protection provisions that may align to some extent with GDPR requirements and provide some level of certainty to EU businesses and individuals while recognizing the limits that privacy legislation would have to address national security surveillance concerns. [...] Although many experts consider legislative changes to U.S. surveillance programs and/or introducing a federal privacy law as options that may go farthest in meeting EU concerns about Privacy Shield, these both could be contentious and complex pieces of U.S. legislation. Views differ across the political spectrum on these issues and would likely take considerable time to reach agreement and enact.²⁰⁷²

But there is yet no immediate solution between the EU and the US, as the US commitments in the EO “will form the basis of the Commission’s assessment in its future adequacy decision”.²⁰⁷³ Such decision would then take months. The initial criticism of the EO is already fueling doubts about a positive outcome of the assessment by the Commission in the run-up to such a decision. Should the existing criticism harden, NOYB has already announced its intention to take legal action: “In the end, the CJEU’s definition will prevail – likely killing any EU decision again”²⁰⁷⁴.

Until then, the legal situation according to *Schrems II* would apply. Companies would not be able to rely on a mere announcement of this new agreement to transfer data to the US in a legally compliant manner but would have to continue to rely on the “appropriate safeguards”, Art. 46 GDPR. Overall, the EU-US DPF could lead to even more legal uncertainty.²⁰⁷⁵ It will also be important, “that whatever senior political leaders wanted in terms of securing a new data transfer agreement would still likely be challenged in Europe’s highest court. With such legal uncertainty looming, it was critical to ensure any new agreement would be in water-tight compliance with the 27-country bloc’s tough data

²⁰⁷¹ Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (31 January 2022). EU/US Adequacy Negotiations and the Redress Challenge: EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an “Essentially Equivalent” Solution. *European Law Blog*. <https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution>.

²⁰⁷² USA, Congressional Research Service. *U.S.-EU Privacy Shield and Transatlantic Data Flows*, R46917, (22 September 2021). P. 22–23.

²⁰⁷³ USA, The White House. *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework>, (25 March 2022).

²⁰⁷⁴ NOYB. (7 October 2022). *New US Executive Order unlikely to satisfy EU Law*. <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>.

²⁰⁷⁵ NOYB. (25 March 2022). *Privacy Shield 2.0? Erste Reaktion von Max Schrems*. <https://noyb.eu/de/privacy-shield-20-erste-reaktion-von-max-schrems>.

protection standards”²⁰⁷⁶. US-based MNEs such as Microsoft have therefore already indicated that they support the EU-US DPF but remain hopeful for a sustainable global solution:

Microsoft will continue to support additional efforts to establish consensus around the globe on the appropriate balance between privacy and security, including through engagement at the OECD and in other global forums. We are committed to helping develop durable global solutions. The new framework agreed to by the EU and the U.S. sets a very high standard for how governments should seek to access Europeans’ personal data and contains important rights for individuals to obtain redress if their data are accessed inappropriately. It is a welcome development and an important achievement for the data protection rights of Europeans.²⁰⁷⁷

The ASEAN Framework on Personal Data Protection contains only three data subject rights, which are the right to access, the right to correct, and the right to be informed. However, the latter only vaguely refers to “information about an organizations policies and practices with respect to personal data [...] and how to contact the organization” about those polices and practices. In addition to the four essential guarantors, the APEC Privacy Framework 2015 contains in para. 20 the “choice principle” to “ensure that individuals are provided with choice in relation to collection, use, transfer and disclosure of their personal information”. However, even the commentary notes of this framework do not provide more precise information on which data subject rights are to be covered by this “choice” and leave too much room for interpretation.

Art. 4 UN Guidelines requires Members States to provide legal protection for a data subject, irrespective of nationality or domicile, and includes the four essential guarantees. Exceptions from Arts. 1-4 UN Guidelines “may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards”, Art. 6 UN Guidelines. Exceptions to Art. 5 UN Guidelines “may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination”, Art. 6 UN Guidelines. Member States should provide, in addition to civil remedies, also criminal or administrative penalties in the event of a breach of the requirements laid down by the UN Guidelines.

As a result of Chapter IX Section III.3, a coverage of the essential guarantees can be identified as follows:

²⁰⁷⁶ Manancourt, V. [Vincent] and Scott, M. [Mark]. (25 March 2022). Political pressure wins out as US secures preliminary EU data deal. *Politico*. <https://www.politico.eu/article/privacy-shield-data-deal-joe-biden-ursula-von-der-leyen>.

²⁰⁷⁷ Brill, J. [Julia]. (25 March 2022). *EU-U.S. data agreement an important milestone for data protection, Microsoft is committed to doing our part*. <https://blogs.microsoft.com/eupolicy/2022/03/25/eu-us-data-agreement-an-important-milestone-for-data-protection-microsoft-is-committed-to-doing-our-part>.

Essential guarantees	US	Europe	China	APEC	ASEAN	UN	OECD
Processing should be based on clear, precise, and accessible rules							
Necessity and proportionality regarding the legitimate objectives pursued need to be demonstrated							
An independent oversight mechanism should exist							
Effective remedies need to be available to the individual							

IV. Conclusive remarks

Egon Bahr, former Minister of the German Federal Government, once said that “international politics is never about democracy or human rights. It’s about the interests of States. Remember that no matter what they tell you in history class.”²⁰⁷⁸ This Chapter IX put its focus on this importance of interests as causal motives for foreign policy action and – based on the multi-stakeholder approach – presented all interests involved as “endogenous variables” in a global ecosystem of TFPD.

“Free flow of personal data” interests can be of different kinds, inter alia for scientific purposes (e.g., research in a foreign University data bank) and law enforcement purposes (e.g., e-discovery). There is also an economic interest involved when seeking to sell or buy services related to personal data. A State may have a vital interest in accessing personal data stored abroad. The interest in free flows of personal data then raises human rights issues such as the freedom of information, freedom of speech, and the right to data protection. Free flow interests are not unlimited. SPs having a preferred market position may want to exclude other SPs from the market, while other SPs seek to enter the market. SPs have an interest in promoting or obtaining respect for the intellectual property concerned and thus in excluding those who are not willing to provide such respect. Political interests may also be involved, for example to protect national security, or the desire not to be dependent on foreign data transfer facilities. There is also a public welfare interest involved, namely the general interest in the development of the economy and in technical innovation. Others are “availability” interests. A primary issue herewith is the availability of facilities involved in TFPD. In the early nineties, such facilities were still rare, especially for high-speed transfers, major factors were therefore the costs of transfer services and standardization (e.g., protocols). The interest of reaching another individual and to be reached by other users affects the availability component in nowadays digital society. Its users have interests in the transfer being reliable, incapable of being intercepted or interfered with and to be secure in terms of data security. Section I of this Chapter IX can – regarding States interests – be summarized by an observation of the UN that is consistent with our findings:

Among developed countries, there is a large, developed country – the United States – hosting global digital platforms with strong market power that favors free cross-border data flows, in order for them to be able to get most of the gains from the data collected in their operations worldwide. Smaller developed countries, whose internal markets are not big enough to benefit from restrictions, tend to favor free cross-border data flows.

²⁰⁷⁸ On 3 December 2013 in conversation with schoolchildren as part of the “Willy Brandt Reading Week” at the Friedrich Ebert House in Heidelberg, Rhein-Neckar-Zeitung, 4 December 2013

The European Union is a particular case, as it privileges privacy and data protection motivations. Among developing countries, those with large domestic markets mostly favor data localization to promote the development of their digital economies. In the case of China, national security motivations also play a major role. For the rest, smaller developing countries, the picture is mixed. Data localization is not likely to be of use, given the small size of their markets, while free cross-border data flows imply giving away a domestic resource without any return.²⁰⁷⁹

China and Russia currently represent special cases. They use their diplomatic and economic power to set standards which generally go against the idea of a free transborder Internet and promote national control. In the long run, this State surveillance would have to evade international control and a global multi-stakeholder approach involving civil actors to work undisturbed. Therefore, these States would follow the approach of “tech-nationalism” rather than a concept of multilateralism. The question of how technologies are applied domestically will play a major role in determining the competition between liberal democracies and digital autocracies.

The endogenous variables were also grouped into three different arenas and related to exogenous variables. Regarding the latter, it can be summarized that these result in three different framework archetypes.

The European framework exercises value-based control over personal data and is fundamental rights oriented. The strategic orientation to increase control of personal data is based on regulatory leadership and partnerships. The transfer mechanism follows a general scope, a transfer is conditional on certain safeguards (prescriptive approach) and has no specific requirements for data flow restrictions. The European framework is advanced and comprehensive according to the GSMA and de Terwangne classifications and thus has the greatest maturity. The comparative law approach in this Chapter IX compares the frameworks in these concluding remarks with the current maximum of the European framework.

The US framework is a mixture of piecemeal/patchwork model and sector-oriented model. In it, the private sector has control over personal data. The strategy to increase control of personal data lies with private digital corporations and is thus trade oriented. The transfer mechanism of the US refers to a sector-specific scope, is based on ex-post accountability (light touch approach) and specifies a local storage requirement only for a few data types. If the US discovers at federal level “that it needs to compete for global influence with its own modern data privacy law, abandoning the pretense that notice and consent is sufficient”²⁰⁸⁰, then the maturity level of the US framework could possibly be raised to European level. For this to happen, the proposed ADPPA would have to be enacted at the federal level. While the CPRA reflects all data protection principles and an essentially equivalent level of protection, this is only State law, and it is uncertain whether it will be the common denominator in the “competition” of US State laws against a less comprehensive Virginia model and other US State law models. Under ADPPA, all data protection principles and, except for the right to restrict processing and the right in relation to automated decision making and profiling, all data subject rights would be guaranteed at the federal level. At least four remedies out of those required by the European framework which need to be available to the individual, namely, the right to be informed, the right to access, the right to correct, and the right to erasure, would be fulfilled. However, this will still be determined by developments in the US arena and the

²⁰⁷⁹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 139.

²⁰⁸⁰ Greenleaf, G. [Graham]. (1 October 2021). China’s Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report*, 2021(172), <https://ssrn.com/abstract=3989775>. P. 6.

EU-US arena. In US federal law, it is not clear whether a statutory or non-statutory approach will be taken. If ADPPA is not enacted, and the EO of 7 October 2022 found to not sufficiently limit surveillance and not to guarantee the required remedy for data subjects, the US framework would not be on an “essentially equivalent” level with the requirements set by *Schrems II* and the proposed EU-US DPF likely to be threatened by an approaching *Schrems III* judgment.

China, as the most influential part of the APAC framework, exercises control over personal data through its government. With its strategic focus on the Digital Silk Road, China is also trade oriented, but with a much stronger government intervention to pursue security rationales. The transfer mechanism in China refers to a sector-specific scope, and to specific data types. China’s data transfer mechanism, which is based on ad-hoc authorization, has a restrictive level and sets requirements for local storage, local access, as well as local processing. Through PIPL, a fundamental rights approach was added for the first time to the rationales of Chinese lawmaking. This is reflected in the coverage of all data protection principles and all data subject rights. However, this still does not mean that Chinese domestic law covers all essential guarantees, as an “independent oversight mechanism” in China is to be doubted. China’s law is since PIPL both sufficiently in the mainstream of GDPR-influenced laws, and sufficiently distinctive that it could become the first significant competitor to the EU in obtaining influence over development of other national data privacy laws in the APAC framework and beyond. Without China, the APAC framework is to be classified as a “progressing level” in a “self-regulatory model”. China alone may well qualify as an “advanced level” in a “comprehensive model”.

The right to data protection no longer represents a particular interest of individual States but is developing into an internationally recognized legal asset of particular importance for the digital society. All frameworks put an emphasis on the objective of “digital sovereignty”. This is due to several factors, such as “the predominance of United States and Chinese companies in the digital technology sector, and the need to reduce dependence on external technologies in the absence of successful European technology companies.”²⁰⁸¹ It also reflects concerns regarding the ability of the domestic market to ensure the protection of personal data of its citizens, and the security risks associated with foreign technologies. All frameworks seek to avoid unnecessary barriers to data flows and to ensure continued trade and economic growth in their respective regions. The international organizations framework, the US framework, and the APAC framework emphasize continued trade and economic growth. In contrast, the European framework focuses on fundamental rights, with the impact on the economy or trade emphasized less. For example, the GDPR seeks to enable “free movement of personal data within the EU while protecting fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”. The APEC Privacy Framework and EU data protection law are both largely based on the OECD Guidelines 2013, and the US is also a signatory State to those Guidelines. New or modernized laws within the US (if proposed initiatives to be included), Europe, and China, are based on common principles, including the recognition of data protection as a fundamental right, the adoption of overarching legislation in this area, the existence of enforceable individual rights to privacy and the establishment of an independent supervisory authority. This offers new opportunities for further facilitating data traffic – in particular through adequacy assessments – while at the same time guaranteeing a continuously high level of protection of personal data.

²⁰⁸¹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 105.

The differences between frameworks are primarily due to the fact that the approach to data protection is always strongly shaped by history and culture. The needs of citizens for protection of their personal data, and their willingness to allow authorities to intervene in this area, vary worldwide. The resulting legal fragmentation is reinforced by the fact that national regulatory authorities tend not to look at international aspects. This is particularly true in an area such as data protection, which has many extensive interfaces with other areas of law and is therefore an intensely challenging subject. Moreover, these authorities face the aforementioned conflicting interests. States will therefore regularly protect economic interests more strongly, whereas countries without significant economic sectors influenced mainly by VLOPs, as is still the case in some EU countries in an international comparison, will prioritize fundamental rights protection. This contributes to the fact that the EU and the US, as important markets for the IT economy, are based on a different and rarely concurrent perception of interests. There are still significant differences between the APEC and EU approaches to data protection and the EU does not accept the US as generally providing an “adequate level of protection” under EU data protection law. At the same time, the importance of State borders for transborder data flows is diminishing since the Internet is being used more and more intensively as a transport medium in countries that have not yet been regulated in the area of data protection.

Recently, the US has moved towards the requirements of the European framework. Besides judicial redress, the CJEU also found US surveillance being not “proportionate” in its scope and operation. The FTC likes to see itself in the role of an independent data protection authority according to the European framework but does not yet fulfill the criteria for the independence of such authority. There are still points to be solved within the US framework to create an “essentially equivalent level of protection” according to the requirements of the CJEU. California State law could hereby create the possibility of greater agreement on federal preemption. Although the CPRA relates only to consumer rights in California, the rules are like those of the GDPR and could serve as a US nationwide role model. Future developments in the US will also depend on the priority the 117th Congress will give to the topic, especially on the approval of the proposed ADPPA. The US is lucky in this case, as they are not yet so far with regulation on the federal level. The EU is far ahead in this respect, perhaps too far, and therefore struggles with a “set theory”, i.e., intersections and therefore the rationales of different instruments. The GDPR nevertheless contains a lot of potential for improving the protection of personal data at global level. Between the US trade-oriented approach and the – in the largest parts – national security-oriented approach of China, the GDPR shows a development path based on elementary fundamental rights such as human dignity. It indicates the direction in which the use of personal data for social, economic, and governmental purposes could be reconciled with the respect for and protection of fundamental rights and freedoms and how to keep pace with technological developments. The GDPR has already a global dimension and serves many countries as a blueprint for a third way of development into the digital world.²⁰⁸² To follow this positive trend of other countries leaning towards the rules of the GDPR, however, negative aspects being immanent in the GDPR outlined above in the “EU arena” must also be considered. As a study by the GSMA also noted, “the divergence between various frameworks may create tensions between countries and regions. Data privacy regulators and stakeholders are today grappling with these tensions, and data privacy frameworks are continually evolving in various attempts to address these challenges.”²⁰⁸³

²⁰⁸² European Commission. *Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock*, COM(2019) 374 final, (24 July 2019). P. 12 ff.

²⁰⁸³ GSMA. (September 2018). *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC can Protect Data and Drive Innovation*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf. P. 19.

In view of these divergences, it is not surprising that little progress has been made at global level in harmonizing data protection law governing TFPD.²⁰⁸⁴

The following Chapter X will therefore address objectives of a regulatory intervention. Returning to what was stated in Chapter I Section II.4.3, “What?”, “When?”, “Where?”, “Why?”, and “Who?” have been answered so far. The question of the “if” of an intervention – because of the existing patchwork situation²⁰⁸⁵, the resulting problems²⁰⁸⁶, and effects on stakeholders²⁰⁸⁷ – is no longer to be answered after what has been established so far. Nevertheless, the questions of “What for?” and “How?” remain for the subsequent Chapter.

²⁰⁸⁴ “Globally there is a general recognition that there should be some law regarding cross-border data transfers, but a wide variety of approaches to this issue exist, and there is no single global model for managing it.”
http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf, page 12

²⁰⁸⁵ Chapters II-VII

²⁰⁸⁶ Chapter VIII

²⁰⁸⁷ Chapters IX

CHAPTER X: OBJECTIVES FOR INTERVENTION

Following the specific methodology of this thesis,²⁰⁸⁸ objectives of an intervention must be defined. These “link the analysis of the problem (and its causes)²⁰⁸⁹ to the options²⁰⁹⁰ for the policy response. They set the level of policy ambition, fix the yardsticks for comparing policy options and determine the criteria for monitoring and evaluating the achievements of implemented policy.”²⁰⁹¹

Objectives are divided into “general”, “specific” and “operational” objectives. General objectives are the “goals which the policy aims to contribute to”, while specific objectives “set out concretely what the policy intervention is meant to achieve. They should be broad enough to allow consideration of all relevant policy alternatives without prejudging a particular solution, i.e., the specific objectives are part of the intervention logic: problem-drivers-specific objectives-policy options.”²⁰⁹² At the end of Chapter XI, based on these general and specific objectives, the “preferred option”²⁰⁹³ will be determined. This option will contain “operational objectives”, which

are defined in terms of the deliverables of specific policy actions. As such, they are typically option-specific. These should not, therefore, be reported in the same place [...] as the general and specific objectives but reported in the section referring to the preferred policy option [which will be Chapter XII]. While general, specific and operational objectives will generally be needed for a legislative initiative, only general and specific objectives will be needed for a communication setting out broad policy objectives. Whereas for implementing legislation, there will be no need to set out general objectives which will have been discussed in the context of the basic act.²⁰⁹⁴

Setting those criteria for objectives should lead to “regulations and related decision-making process [remaining] transparent, non-discriminatory, efficient, in line with the stated public policy objectives and better integrate consideration of market openness principles (including avoidance of unnecessary trade restrictiveness).”²⁰⁹⁵

In the elaboration of the objectives, it is not relevant whether they are influenced by the private sector and/or the public sector, whether the objectives overlap between both sectors, or are the same. A separation between public and private actors was important above in Chapter IX to present the stakeholder interests underlying the following

²⁰⁸⁸ Chapter I, Section II.4.3.

²⁰⁸⁹ Chapter VIII.

²⁰⁹⁰ Chapter XI

²⁰⁹¹ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 100.

²⁰⁹² European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 100.

²⁰⁹³ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 100.

²⁰⁹⁴ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 100.

²⁰⁹⁵ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Para. 32.

objectives. In this Chapter X, however, the objectives of an intervention with a focus on a solution for all stakeholders will be discussed. The aim of this Chapter is also to determine which objectives could be realized at all. The results of Chapter IX are helpful in this respect, as they identified which “minimal positions” for a consensus on an intervention exist and in which frameworks these positions are located.

The problem analysis and the impetus (Chapter VIII), and the assessment of the stakeholder interests (Chapter IX), must now be followed by an impact assessment which also includes a risk assessment in a broader sense. Essentially, the general objective – accompanied by the specific objectives – should serve to solve the aforementioned²⁰⁹⁶ core problem, that is, the dilemma of a free flow of personal data vs. restrictions on the free flow of personal data. Since the problems are known at this point of this thesis, this risk assessment is not a mere “precautionary and preventive principle” against still uncertain consequences,²⁰⁹⁷ but is also determined by the principle of “scientifically guided evidence”,²⁰⁹⁸ both complementing each other. This means that a free flow of personal data should in principle be encouraged if there is no scientific evidence that this free flow is likely to cause harm.

The objectives in this Chapter are therefore not only to focus on risk prevention, but to consider the benefits of the free flow of personal data. There is also a trade-off involved. If, after weighing, we come to the conclusion that the free flow of personal data is beneficial to the rights of individuals and thus to society, despite the potential risk, scientifically guided evidence comes into consideration; if, on the other hand, after weighing, we find that the risk of this free flow outweighs the positive effects, the precautionary and preventive principle comes into play in order to limit this free flow in regulatory terms.

I. General objective

The general objective is that an intervention, in the interest of effective protection of fundamental rights, harmonizes the existing data protection regulations at the highest possible international level and reduces existing barriers to the free flow of personal data, which should enable the digital economy to operate efficiently and deliver benefits more rapidly in multiple nations and regions.

To enable this – following an official T20²⁰⁹⁹ Policy Brief – “the benchmark model is the microeconomic model under perfect competition in which the laissez-faire economy achieves the Pareto efficient equilibrium. The implication is that without market failure, the economy can achieve the highest welfare. There is a presumption that free flow is consistent with optimal outcomes.”²¹⁰⁰ This means that an intervention should aim at the best possible state in which it is not possible to improve one objective without at the same time worsening another. Ultimately, this is about maximizing the general benefit, a social optimum, that is, a focus on comfort and efficiency that consumers and users can

²⁰⁹⁶ Chapter VIII, Section IV.

²⁰⁹⁷ Birger, A. [Arndt]. (2012). Das Risikoverständnis der Europäischen Union unter besonderer Berücksichtigung des Vorsorgeprinzips. In L. [Liv] Jaeckel and G. [Gerold] Janssen, *Risikodogmatik im Umwelt- und Technikrecht* (pp. 35–50). Mohr Siebeck. P. 36–39.

²⁰⁹⁸ Hilf, M. [Meinhard] and Oeter, S. [Stefan]. (2010). *WTO-Recht, Rechtsordnung des Welthandels*. Nomos. § 19 No. 21.

²⁰⁹⁹ Think 20 (T20) is the research and policy advice network for the G20 to drive policy innovation to help G20 Leaders address pressing global challenges and seek a sustainable, inclusive and resilient society. In 2019, the T20 was convening in Japan under Japan’s G20 presidency.

²¹⁰⁰ Chen, L. [Lurong] et al. (29 March 2019). *The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies*. <https://t20japan.org/policy-brief-digital-economy-economic-development>. P. 4.

enjoy. The specific objective of a human-centric approach (see below, Section II.3) also correlates with this idea.

Weber found that “from a theoretical perspective, the harmonization of data protection standards would certainly facilitate the transborder flow of information. Globally, this objective cannot be achieved in a foreseeable future, but harmonization has made some progress on a regional level, for example within the members of the European Union.”²¹⁰¹ It is possible that the objective of harmonization will take longer than this “foreseeable future”. Nevertheless, harmonization is without alternative as a general objective because of the reasons found in Chapter VIII.

Aaronson stated that through harmonization, shared rules are to be achieved, whereby “the internet would [then] be less likely to fragment, more people would have greater access to information and individuals could create and share more information. Individuals might also be better able to obtain rents from their personal data and have some modicum of control over its use.”²¹⁰²

As already explained above²¹⁰³, we are not seeking standardization or full unification but “only” a harmonization of data protection law by globally binding rules directly applicable. However, it is desirable for an intervention to find stricter rules for the parts²¹⁰⁴ to be regulated that are essential for a free flow of personal data and the protection of fundamental rights, which then would come close to standardization. The objective is to avoid fragmentary harmonization “which creates tiny islands of unified law in a sea of national law, [...] especially when these islands are surrounded by a broad zone of which it is impossible to say whether it is still a coast or already a sea”.²¹⁰⁵ The principle of subsidiarity must also be observed in legal harmonization; if decentralized rule formation leads to satisfactory results, harmonization must be avoided.²¹⁰⁶ For the further course of this Chapter, the harmonization within the European framework can serve as an example, also because it follows a human-centric approach with a focus on fundamental rights protection, which is a specific objective to be explained in more detail below²¹⁰⁷. Von Arnould correctly noted that “a cautious and balanced unilateralism – especially on the part of the EU and its Member States – could provide an important impetus in this respect to establish a much-needed global right to digital privacy.”²¹⁰⁸

By eliminating unnecessary localization measures, the costs of closing off national markets with data protection regulations, which were presented above²¹⁰⁹ as a problem for the information society and the digital economy, would be reduced. Governments should be required to facilitate such flows and eliminate unnecessary localization measures to reap the benefits of free data flows for individuals, businesses, and

²¹⁰¹ Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130. P. 121.

²¹⁰² Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 3.

²¹⁰³ Chapter I, Section 4.

²¹⁰⁴ These are reflected in the analysis of the specific objectives in Chapter X, Section II.

²¹⁰⁵ Kötz, H. [Hein]. (1986). Rechtsvereinheitlichung – Nutzen, Kosten, Methoden, Ziele. *Rebels Zeitschrift für ausländisches und internationales Privatrecht*, 50(1), 1–18. P. 12.

²¹⁰⁶ Kötz, H. [Hein]. (1986). Rechtsvereinheitlichung – Nutzen, Kosten, Methoden, Ziele. *Rebels Zeitschrift für ausländisches und internationales Privatrecht*, 50(1), 1–18. P. 12.

²¹⁰⁷ Chapter X, Section II.3.

²¹⁰⁸ Von Arnould, A. [Andreas]. (2016). Freiheit und Regulierung in der Cyberwelt: Transnationaler Schutz der Privatsphäre aus Sicht des Völkerrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 1–34). C.F. Müller Verlag. P. 23.

²¹⁰⁹ Chapter IX, Section I.

governments. Svantesson also found that for the future of online data privacy, it is necessary to avoid reactions

similar to what we have seen in the context of cross-border defamation law and cross-border anti-competition law where the result has included defensive actions such as laws that prohibit the giving of evidence and the production of documents in foreign proceedings, laws that aim to block or prevent the enforcement of foreign judgments, laws prohibiting compliance with orders of foreign authorities, and claw-back laws.²¹¹⁰

However, there must be some limits to a free flow of personal data. Exemplarily, MNEs can be subject to several legal frameworks even in their activities of daily routine, whereby the question of which of the frameworks is relevant in a TFPD scenario is often not easily answered due to different archetypes. The lack of a sufficient international system,²¹¹¹ coupled with divergent archetypes²¹¹² to data protection regulation could therefore pose severe problems for the practice of data controllers. Another exemplary problem is

increasing power imbalances and inequalities. Cross-border data flows cannot work for people and the planet if a few global digital corporations from a few countries are able to capture most of the gains. Market mechanisms alone cannot lead to efficient or equitable outcomes. Thus, there is a role for public policymaking to maximize the gains from data and cross-border data flows, minimizing the risks involved, while ensuring an equitable distribution of the gains from cross-border data flows. Given the global reach of cross-border data flows, this will involve both national measures and policymaking at the international level.²¹¹³

These problems must be prevented or eliminated whilst maintaining a maximum possible degree of free data flow. The goal should be to protect personal data that is deemed sensitive, rather than mandating its localization, which should include the specification of particular treatment for specific types of personal data. Governments should consult with stakeholders on how to interpret and implement such measures to restrict such flows in particular; the involvement of such stakeholders will be described below²¹¹⁴. Achieving this elimination of unnecessary localization measures will require, as Ustaran noted,

creativity and determination. From developing processes to replicate data at a local level to actively engaging local partners, showing some willingness to find practical ways to meet the requirements will go a long way towards addressing the political and economic drivers behind this trend. That should not mean giving up on data globalization and the benefits that it brings. That is where determination comes in. Both technological development and the human instinct to explore our limits are on our side. But ultimately, our commitment and perseverance to ensure that global data protection becomes a reality will demonstrate that data localization and economic nationalisms are not the answer to the problems we face.²¹¹⁵

²¹¹⁰ Svantesson, D. J. B. [Dan Jerker B.]. (2015). The (uncertain) future of online data privacy. *Masaryk University Journal of Law and Technology*, 9(1), 129–153. P. 140.

²¹¹¹ Chapters II-VII

²¹¹² Chapter IX, Section III.1.

²¹¹³ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 92.

²¹¹⁴ Chapter X, Section II.1.

²¹¹⁵ Ustaran, E. [Eduardo]. (16 June 2022). *In search of a data localization strategy*. <https://www.linkedin.com/pulse/search-data-localization-strategy-eduardo-ustaran>.

II. Specific objectives

1. Consensus

Global rules are not at the beginning, but rather at the end of legal development. Until then, legislation affecting data protection in the broader sense and TFPD in the narrower sense is a matter for the States, which are in competition with each other in terms of regulatory systems and cultural diversity. Individual States have led the way with their own regulations. Others have followed their example or rejected it. This development promoted the global formation of wills on possible solutions to problems. However, as long as significant cultural and legal differences exist, unification that does not take them into account is not desirable, as this would cause too many conflicts. However, this does not preclude mutual legal adjustment through gradual convergence of fundamental interests.

Theories of international socialization, based on such convergence, through a coalescence and interdependence of civil societies have yet no strategic vision beyond the displacement of States.²¹¹⁶ It is therefore necessary to formulate or interpret rules of international law within a comprehensive strategy of international law. Such a strategy is to be understood as the use of means permissible under international law to manage conflict situations.²¹¹⁷ Such a strategy should not only include legal elements, but also technological, market-based, and human-centric responses (blended governance approach)²¹¹⁸. It should also consider the interests of all stakeholders involved (multi-stakeholder approach)²¹¹⁹. Otherwise, such intervention could withdraw the Internet its intrinsic nature and social potential.

Within the global ecosystem of transborder data flows,²¹²⁰ the inclusion of all representatives of the “network community” is therefore essential. One can learn here from the debate on transnational law.²¹²¹ A multi-stakeholder setting such as the Internet, with various conflicting, competing, but also parallel and common interests, calls for a regulatory culture in which regulation and self-regulation, as well as unilateral, plurilateral and multilateral elements, are not in competition with each other but can interact. UNCTAD also stated that “policymaking for global data governance needs to take a holistic, multidimensional, whole-of-government, multi-stakeholder approach, at the national and international levels.”²¹²²

The objective should be to develop an operational multi-stakeholder regime with the involvement of a “critical mass” of stakeholders. This critical mass was described above in Chapter IX. To reach consensus among them, as the first specific objective of this Chapter, the networking of governmental and non-governmental stakeholders is crucial. An intervention should be fundamentally designed to avoid conflict between them. However, given the effort required to harmonize data protection rules at the global level, conflicts between national data protection rules will be unavoidable, at least in the medium term. Accordingly, an intervention does not necessarily have to be conflict-free but should rather use its regulatory claim as a positive force for securing data protection rights worldwide and use the resulting unavoidable conflict to strengthen harmonization

²¹¹⁶ Herdegen, M. [Matthias]. (2019). *Der Kampf um die Weltordnung*. C.H. Beck. P. 23.

²¹¹⁷ Herdegen, M. [Matthias]. (2019). *Der Kampf um die Weltordnung*. C.H. Beck. P. 22

²¹¹⁸ See Chapter I, Section II.4.

²¹¹⁹ See Chapter I, Section II.4.

²¹²⁰ See Chapter IX

²¹²¹ See Chapter I, Section II.5.5.

²¹²² UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 92.

efforts. Such conflicts are minimized in the European frameworks' harmonized area, but consensus building appears difficult globally.

To be able to determine a basis for consensus, we rely on the approach of Cory / Atkinson. They determined a “four-cell typology of issues where there can and cannot be consensus and policy issues that involve public benefits and public harms”.²¹²³

	Opportunity to Develop International Agreements	
	Consensus	No Consensus
Desirable	Universal Goods	Local Goods
Undesirable	Universal Bads	Local Bads

Source: Atkinson, Robert D. / Cory, Nigel, “Typology of Internet policy goals affecting individuals outside the country”²¹²⁴

An intervention should therefore include the determination of “universal goods” and “universal bads”. Universal bads should justify data flow restrictions in an intervention. Farrell disagreed – and we do too – with the view that while non-state actors may provide at least some common goods, it is unlikely that these forms of provision can be generalized in any meaningful way, that globalization makes it vastly more difficult to solve international common good problems, and that the capacity of States to respond to these problems is ever weaker.²¹²⁵ We find – with Farrell –, that

States may still try to solve collective action problems through unilateral action, through coordination among themselves, and through new forms of policy which mix public and private action. The second and third of these types of solution typically require negotiations which seek to harmonize forms of common good provision across arenas, or at least to ensure the compatibility of different solutions in different arenas. This layer of international negotiation provides new opportunities for actors in domestic arenas.²¹²⁶

Stakeholders will need to make trade-offs between the benefits, depending on their development goals. A new data governance approach for policy makers is needed that balances the desire for sovereignty with the need for global and cross-sectoral cooperation. This also requires improving our understanding of this trade-off. European heads of State such as former German Chancellor Merkel and French President Macron also made this point.

The fact that senior European policymakers think that data stored on a foreign cloud service represents lost sovereignty shows how little some understand how firms

²¹²³ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 225.

²¹²⁴ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 226.

²¹²⁵ Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US 'Safe Harbor' Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield. P. 101.

²¹²⁶ Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US 'Safe Harbor' Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield. P. 101.

manage data, and how much they prioritize this misguided sense of control. Europe tries to position itself as a moral leader of digital regulation, using concerns over data protection and artificial intelligence (AI) to cloak their discriminatory and restrictive policies. Europe's protectionist intent appears in nearly every digital policy proposal. Europe's GDPR is evolving into the world's most significant de facto data localization framework. Europe's draft data strategy pushes for data localization and asserts that the EU needs cloud providers owned and operated in Europe. Likewise, Europe's white paper on AI advocates data localization precepts. It is also evident in the proposal for a European cloud via GAIA-X.²¹²⁷

An intervention would have to consider the interests pursued, while minimizing the negative effects associated with the exercise of regulatory sovereignty. A solution to the question of the permissible exercise of regulatory sovereignty should therefore consider, on the one hand, the understandable desire of States for sovereignty and, on the other, the desire of individuals to be granted effective protection of their personal data. In this respect, an intervention must also be measured against the requirement to balance interests. Already in 1980, the group of experts entrusted with the preparation of the OECD Guidelines 1980 considered in the related question of applicable law that the optimal protection of a data subject should be at the center of the considerations. The Explanatory Memorandum to the OECD Guidelines 1980 stated therefore that a consensus on data privacy principles "would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws"²¹²⁸. An intervention will have to be measured against whether it can ensure this protection of data subjects effectively and globally.

2. Universality

It was noted above²¹²⁹ that stakeholders of a regulatory process have different rationales for different policies to regulate TFPD. Someone might argue that supranational regulations in a certain region are preferable to those of a universal approach, because the former might have the advantage of being responsive to regional specificities, because there is inclusion in a geographic area and inevitably increased communication, common historical and cultural heritage, and because identical or similar political ideas of State formation, evolved economic and trade relations as well as other homogeneity-promoting links could form a suitable basis especially for treaties whose object is the protection of human rights. But this would oppose rules as universal as possible.

Moreover, a regional approach would lead to harmonization in this area of law too late, if at all. Cory / Atkinson / Castro found that

nations have different values and priorities, and attempts at resolving policy disputes inevitably falter because the various Parties lack a common basis for dialogue. This leads to two generally opposed approaches: universalism and Balkanism. Regarding the former, a reason many proposed frameworks have failed is they try to apply a particular nation's worldview, such as promoting democracy and freedom of expression (as in the case of the United States), or maintaining political control (as in the case of nations such as China and Russia), on the rest of the world. However, some of the

²¹²⁷ Chazan, G. [Guy]. (12 November 2019). Angela Merkel urges EU to seize control of data from US tech titans. *Financial Times*. <https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca>.

²¹²⁸ OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum*, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#preface>. Para. 8.

²¹²⁹ Chapter VIII

most fervent calls for universalism come from cyber-libertarian groups in the West [...].²¹³⁰

We follow this “cyber-libertarian” view and determine universality as the second specific objective. Above²¹³¹ we described that within the framework of the “architecture for global data governance” of the WEF, certain governance “elements” can be assigned to a “universal availability”. In principle, only these elements should be included in an intervention. However, it is possible that certain elements, which are to be assigned to a “limited participation”²¹³², are necessary for the intervention; these can include in particular certain transfer mechanisms. This mixture of mainly universality with certain elements of regional specificity is due to two approaches described above²¹³³: the “blended governance approach” and the “multi-stakeholder approach”.

It is mainly the transfer mechanism that drives the question whether a governance approach is “universal” or “limited”. Since we are aiming at universality, it is necessary to examine which transfer mechanism should be determined as a specific objective in an intervention. The aim must be to include only those mechanisms for which the maximum possible consensus could be reached in an intervention. This consensus also depends on the national policy capabilities outlined above²¹³⁴, which have been assigned to these areas of a State’s regulatory interest: Security Policy, Economic Policy, Infrastructure Policy, and Legal Policy.

The systematics of the WEF determined “unilateral openness”, “legitimate grounds” and “accountability-based” as belonging to the element “transfer mechanism” with “universal availability”.²¹³⁵ Unilateral openness (no restrictions imposed) is to be rejected from the outset since it would not change the current situation of a fragmented global regulatory landscape which leads, inter alia, to problems for individual’s fundamental rights protection. The other sub-elements of the element “transfer mechanism” within the WEF systematics are to be discussed further.

The scope of application of such a mechanism can be either “general”, “sector specific”, or “data type specific”. TFPD are common to most sectors.²¹³⁶ A sector specific approach is therefore to be rejected, as it could entail too great a risk of a renewed patchwork solution and run counter to the general objective of harmonization.

However, it is possible to deviate from the general scope of application for certain data types if a consensus for an intervention could only be found that way. China would have a strong interest in not deviating significantly from its data governance system elaborated since 2017 via CSL, DSL, PIPL and various measures and specifications. This system is based, in this way for the first time on a global level, on a not *per se* detrimental classification of data types according to their impact on national interests (e.g., “core data”). Not unique at the global level but common to all frameworks is the recognition that for sensitive personal data special rules must exist for transborder transfers of such data types. Similarly, the interests of the “national digital economy / economic development lens”, the “national security / public order / sovereignty lens”, and the “adequacy and gaps in coverage / citizens’ protection lens” are recognized as conflicting

²¹³⁰ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²¹³¹ Chapter IX, Section III.1.4.

²¹³² Chapter IX, Section III.1.4.

²¹³³ Chapter I, Section II.4.

²¹³⁴ Chapter IX, Section I.2.1

²¹³⁵ Chapter IX, Section III.1.4.

²¹³⁶ Chapter IX, Section III.1.4.1.

with a free flow of personal data.²¹³⁷ To this end, certain types of data could be excluded from a free flow altogether or their transfer limited but regulated differently than for sensitive personal data.

It was found above that data flow restrictions are not beneficial to the pursuit of the rationale of “national digital economy / economic development”, but rather have the opposite effect.²¹³⁸ Moreover, it may lead to conflicts with GATS, should a State base such restrictions on the rationale of the digital economy.²¹³⁹ A transfer mechanism that limits the free flow of personal data based on this rationale should therefore be disregarded in an intervention.

Part of the general objective of an intervention is harmonization, which will ideally eliminate the fragmentation of regulations altogether.²¹⁴⁰ The “search for legal mechanisms that will ensure adequacy of protection and, at the same time, will not create barriers to the development of global digital services”²¹⁴¹, which had become difficult until such a proposed intervention, would then be over. It would then make no difference in which countries the data processing takes place as the same data protection principles²¹⁴² and essential guarantees²¹⁴³ would apply. This would prevent the protection of data subjects from weakening when the geographical scope of these processing activities is expanded. Personal data would then be protected essentially equivalent when transferred internationally. This would eliminate the misconception that data stored in a national market is more secure than data stored internationally, not the least by improving trust²¹⁴⁴. Data flow restrictions through the classification of diverse data types based on the “adequacy and gaps in coverage / citizen protection” rationale can therefore be excluded in an intervention.

The rationale of “national security / public order / sovereignty” is more diverse and requires a closer look. In this regard, UNCTAD stated that

in principle, a large number of measures that countries are taking to restrict cross-border data flows can be justified through security or public moral reasons. Data localization measures, for example, that require domestic storage of data are often adopted on security grounds, whether for national security or to limit foreign surveillance. The public interest in the issue of cross-border data flows has, for example, increased following the publications of the revelations of former analyst of the National Security Agency of the United States Edward Snowden, alleging that the agency and other surveillance agencies were engaged in massive global online surveillance. This undermined the privacy of many individuals in the United States and abroad, leading some countries to adopt strategies to restrict the flow of data.²¹⁴⁵

Other regulations besides PIPL also use “national security / public order / sovereignty” as justification for exceptions. Convention 108+ cites “the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other

²¹³⁷ Chapter VIII, Section I.

²¹³⁸ Chapter VIII, Section I.1.

²¹³⁹ Chapter VIII, Section I.1.

²¹⁴⁰ See Chapter X, Section I.

²¹⁴¹ Rojszczak, M. [Marcin]. (2020). CLOUD act agreements from an EU perspective. *Computer Law & Security Review*, 38 (2020), <https://doi.org/10.1016/j.clsr.2020.105442>. P. 1.

²¹⁴² Chapter IX, Section III.2.

²¹⁴³ Chapter IX, Section III.3.

²¹⁴⁴ See Chapter X, Section II.5.

²¹⁴⁵ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 148.

essential objectives of general public interest”, the GDPR “important reasons of public interest”, the ECHR “national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”, the proposed ADPPA that the “transfer is necessary to prevent, detect, protect against, or respond to a public safety incident, including trespass, natural disaster, or national security incident.” The international organizations framework also mentions these. “Internal and external security” plays an important role through Art. 19(3b) ICCPR. The OECD noted that measures under this rationale take place “either in terms of protection of information deemed to be sensitive, or the ability of national security services to access and review data. The latter in particular can be very broad in nature, providing wide scope of access to any form of data”²¹⁴⁶. Law enforcement purposes also fall under this rationale of sovereignty.²¹⁴⁷ Above²¹⁴⁸ it was described that a State has both positive and negative obligations to protect its citizens. In its positive dimension, which is newer in the development of international law, a State has the duty to enact regulations and to enforce them (even against foreign actors).²¹⁴⁹ Law enforcement purposes therefore can form the justification for exceptions to a free flow of personal data in regulatory instruments. The GDPR states that the “establishment, exercise or defense of legal claims” may constitute a derogation for certain situations. Art. 8 ECHR includes a defensive function, which consists in the establishment of effective judicial protection and the implementation of measures to protect the rights of individuals. One of the positive obligations to act is that each Party to the ECHR must ensure laws that give the affected individuals the opportunity to defend themselves in a fair trial against interference of their rights and provide sufficient procedural guarantees that enable affected individuals to effectively challenge interferences through legal action. Cory / Atkinson / Castro argued that legitimate law enforcement concerns can be solved by pushing “for new mechanisms [...], while also working to improve the existing mechanisms (such as MLAT 2.0 agreements) many countries rely upon”²¹⁵⁰. States have a legitimate interest in having sufficient legal standards and mechanisms in place for facilitating legitimate law enforcement requests for TFPD through access to those data. Solving this via data flow restrictions is in principle the worse option because of the aforementioned²¹⁵¹ consequences of such restrictions. In particular, a “tipping point” is to be avoided “whereby enough countries doing it [data localization] would make cross-border cooperation on law enforcement investigations that much harder for everyone”²¹⁵². There would therefore be no consensus for an intervention, should such an intervention attempt to exclude data flow restrictions which are based on the “national security / public order / sovereignty” rationale. A general scope of transfer mechanism, with restrictions on certain data types allowed under certain circumstances based on the rationale of “national security / public order / sovereignty”, is therefore preferable within the specific objective of universality. The GDPR offers that derogation, but not as a blanket, as those responsible must be able to show that the derogation is required for the purposes of safeguarding these rationales. We remind at this point that there is no exemption from having a lawful basis for the data processing as such in place, so that a processing of personal data is more generally lawful; there is no exemption from the requirement to process lawfully (first stage test²¹⁵³).

²¹⁴⁶ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 15.

²¹⁴⁷ See Chapter VIII, Section 1.2.

²¹⁴⁸ Chapter IX, Section I.2.1.

²¹⁴⁹ Chapter IX, Section I.2.1.

²¹⁵⁰ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²¹⁵¹ Chapter VIII, Section I.

²¹⁵² Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²¹⁵³ Chapter II, Section II.3.4.4.a.

The ex-post accountability (light touch) approach was described above²¹⁵⁴ as ranking at the lower end in terms of its level of restrictiveness; the “conditional on safeguards” approach represents the middle of the spectrum; the “ad-hoc authorization” approach the most restrictive level. Cory / Atkinson / Castro examined a “data free flow with trust” approach and found that a necessary principle is accountability.²¹⁵⁵ They argued that this solution should entail that “companies doing business in a country should be responsible and held accountable under that nation’s laws and regulations, for both their own actions and the actions of their agents and business partners, regardless of whether they’re located inside or outside the country where a firm collects or manages data.”²¹⁵⁶ The country responsible for determining that such companies “are legally responsible for any failures to manage data (such as personal data) from that country, regardless of whether those failures are the fault of the firm in that country or abroad, or an affiliate or business partner in that country or abroad”²¹⁵⁷ should be determined by what they called a “legal nexus” in a country’s jurisdiction. The argument in favor of this approach is that it would enable a relatively free environment for TFPD and therefore meet one part of the general objective. It would also fit within the WEF²¹⁵⁸ system. Moreover, the accountability-based approach is shared by most nations – these include the US in particular – and could arguably achieve broad consensus regarding this free flow objective alone. However, this would neglect the fact that data subjects who do not reside in the very country of this “legal nexus” but enjoy a higher level of protection for personal data in their home country, could have their fundamental rights compromised. This has been demonstrated, for example, by the weaknesses of Safe Harbor and Privacy Shield and related disputes in the EU-US arena²¹⁵⁹. Cory / Atkinson / Castro presumably saw this problem as well, as they also noted that “in this case, the only way nation A’s [where the legal nexus is] laws can be enforced – whether or not they require data localization – is if they simply cut off their citizens’ access to all foreign websites”²¹⁶⁰. However, such an approach would not minimize the negative effects associated with the exercise of national sovereignty but would result in the application of a national law to a TFPD scenario that could potentially encompass all countries in the world. Moreover, the broad recognition of the accountability principle at global level applies only to the data processing activity as such (first stage test)²¹⁶¹, not to the same extent to a transfer mechanism (second stage test)²¹⁶². Cory / Atkinson / Castro further described that for the accountability principle to succeed, “interoperable privacy frameworks [as] the international extension of this accountability-based approach” are needed so that “such that data is still able to flow between different privacy regimes, and countries data protection rules flow with it”.²¹⁶³ We also believe that a specific objective should be a policy coordination to resolve jurisdiction and enforcement issues in an intervention. However, one would have to distinguish between those States that would be bound by an intervention and those that would not. For the former, the accountability approach can still be a specific objective²¹⁶⁴

²¹⁵⁴ Chapter IX, Section III.1.4.1.

²¹⁵⁵ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²¹⁵⁶ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²¹⁵⁷ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²¹⁵⁸ Chapter IX, Section III.1.4.

²¹⁵⁹ Chapter IX, Section II.1.

²¹⁶⁰ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²¹⁶¹ Chapter II, Section II.3.4.4.a.

²¹⁶² Chapter II, Section II.3.4.4.a.

²¹⁶³ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²¹⁶⁴ See Chapter X, Section II.6.

as well as an operational objective²¹⁶⁵, as it would be supported by a uniform substantive ruleset. For TFPD between in-scope countries and the rest of the countries worldwide (“scenarios with external relationship”), an ex-post accountability approach as a transfer mechanism is not ambitious enough and indeed a “too light touch”.

A flow conditional on safeguards, also called “prescriptive approach”, exhibits a high degree of flexibility; on the one hand, through the range of possible safeguards, the scope of which was most extensively demonstrated by the GDPR; on the other hand, also through the possibility of determining who sets the requirements for these safeguards and in which process. Depending on how the requirements differ in quantity and quality, transfers conditional on safeguards can also be distinguished in particular in their impact on those responsible for such transfers.²¹⁶⁶ The European framework and now also China follows the three-tier mechanism, which stipulates the transfer requirements from three aspects: adequacy, safeguards, derogations. However, China deviates from this in that adequacy is not determined for the recipient country as such, but only for certain transfers of a data exporter; also, transfers of certain data types are made dependent on an ad-hoc authorization; moreover, the derogations are not determined with sufficient legal certainty.²¹⁶⁷ Nevertheless, a prescriptive approach offers a greater likelihood of consensus because it is the most frequently used in practice.²¹⁶⁸ A prescriptive approach would therefore need to be incorporated into the specific objective of universality. The question, however, is to what extent an intervention should deviate from a prescriptive approach to approximate China’s restrictive approach to build consensus. PIPL includes both an adequacy recognition to be conducted by data exporter (PIPIA) and one based on the perspective of a sovereign rights holder, the CAC-led assessment.²¹⁶⁹ The former is mandatory for all cases of Art. 38(1)-(3) PIPL, while the latter is for the case of Art. 38(1) PIPL. The former is similar to the TIA of the GDPR, while the latter is close to an adequacy recognition process of the European Commission.²¹⁷⁰ Thus, there is nothing to object to the Chinese approach as such. Also, as noted above, there is in principle nothing to object to subjecting certain types of data, which can be verifiably demonstrated to fall under the “national security / public order / sovereignty” rationale, to ad hoc authorization. The GDPR (as well as Directive 95/46) is also familiar with such ad hoc authorizations: Art. 46(3)(a) GDPR allows the creation of specific transfer agreements between exporter and importer, subject to authorization from the competent SA; Art. 46(3)(b) GDPR permits transfers based on administrative arrangements made by the data exporter, subject to the authorization from the competent SA. Problematic in the Chinese approach, however, is Art. 38(4) PIPL, which states that “[...] where it has satisfied other conditions prescribed by laws, administrative regulations, or the State cyberspace administration”; as well as the vague wording in the PRC Security Assessment Measures “[...] other matters that the CAC considers necessary to assess”, which gives the CAC broad discretion.²¹⁷¹ These discretionary powers contradict an essential principle of the European legal framework, namely “Guarantee A - Processing should be based on clear, precise and accessible rules”, which derives from Arts. 7, 8, 47 and 52 of the Charter, the case law of the ECtHR on Article 8 ECHR and the essential guarantees identified first by the WP29 and later by the EDPB.²¹⁷² Such a discretionary power for a local/national SA (e.g., in China) can

²¹⁶⁵ See Chapter XII, Section III.1.

²¹⁶⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 126.

²¹⁶⁷ Chapter IV, Section IV.5.

²¹⁶⁸ Chapter IX, Section III.1.4.1.

²¹⁶⁹ Chapter IX, Section III.1.4.1.

²¹⁷⁰ Chapter IV, Section IV.5.

²¹⁷¹ Chapter IV, Section IV.5.

²¹⁷² Chapter IX Section III.3

therefore not be included in an intervention. This could create tension (e.g., with China) in the consensus-building process²¹⁷³. Atkinson / Cory noted that

China should revise its restrictive approach to data and digital policies so that it can play a constructive role in debates and negotiations between like-minded countries. If China retains its restrictive approach to data, AI, and digital trade, it will increasingly find itself excluded or marginalized in global discussions on digital issues as other countries will see its approach as far from the baseline of emerging global norms and as self-serving (and not mutually beneficial) from a trade perspective.²¹⁷⁴

We consider this too drastic a view, which unfortunately is readily shared in other sources as well. These do not sufficiently consider that the development of the data protection framework in China, even from a “cyber-libertarian” perspective of the western hemisphere, has made significant progress and has come close to the GDPR as the highest global standard at the present time. The GDPR also works to this day with opening clauses, which allow the Member States a – partly quite vaguely formulated – possibility to deviate in certain cases from the GDPR. This point was also raised by the US side as a criticism in the course of the discussions on a Privacy Shield 2.0.²¹⁷⁵ In fact, national security is not an EU competence, which is why EU Member States can retain sovereignty over national security policy and – this is disputed – the CJEU therefore could have no authority over the surveillance practices of EU Member States. The US Congressional Research Service therefore argued that “in fact, GDPR uses the threat of withdrawing access to EU personal data as a tool to seek reform of other country’s security agencies to reflect the CJEU notion of proportionality, while exempting member state governments from similar expectations or threats”²¹⁷⁶. The discretion within PIPL and PRC Security Assessment Measures is also understandable from a political point of view, at least insofar as one considers the rather short five-year time span of the creation of the advanced and comprehensive framework²¹⁷⁷ for data protection in China. Also, various rules in PIPL have only been sufficiently interpretable since 2022 through the three measures mentioned above²¹⁷⁸ (apart from the still not satisfactorily specified “important data” types). It may therefore be a tactical consideration on the part of the Chinese legislator to leave open adjustments to the transfer mechanism through these vague clauses. The line to be drawn for the content of an intervention at stake should nevertheless be the “essential guarantees”, which are discussed below²¹⁷⁹ as a further specific objective.

The type of data flow restriction also determines whether an intervention is “universal” or “limited”. Such restrictions are an increasing way for nations to assert data sovereignty. There are the options of a local storage requirement, a local storage and processing requirement, or a ban on transfer; the latter imposes local storage, local processing, and local access.²¹⁸⁰ Although the GDPR does not explicitly stipulate such a data flow restriction, its extraterritorial reach causes a *de facto* restriction.²¹⁸¹ These types of data flow restrictions are associated with the level of restrictiveness already explained in this Section II. A conditional flow regime, as stated above as a preferable variant, may well

²¹⁷³ Chapter X, Section II.1.

²¹⁷⁴ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 229–230.

²¹⁷⁵ See Chapter IX, Section II.1.

²¹⁷⁶ USA, Congressional Research Service. *U.S.-EU Privacy Shield and Transatlantic Data Flows*, R46917, (22 September 2021). P. 17.

²¹⁷⁷ Chapter IX Section III.1.5.

²¹⁷⁸ Chapter IV, Section IV.5.

²¹⁷⁹ Chapter X, Section II.3.

²¹⁸⁰ Chapter VIII, Section I.

²¹⁸¹ Chapter VIII, Section I.

contain data flow restrictions. On the one hand, the conditions can apply to the recipient country, on the other hand to the data controller or data processor.

A free flow of personal data has been determined as a general objective of an intervention. However, this flow cannot be unlimited, as soon as it reaches the limits of data sovereignty, and the fact that nations want to exercise control over personal data through assertions of geopolitical power, international agreements about sovereignty recognition, and domestic policy creation. It has already been found (see Chapter VIII, Section I.) that the “national security / public order / sovereignty” rationale can be a justifiable limitation, as long as the justifications restrictions of TFPD based on this rationale are based on clear, precise and accessible rules; nor may these be applied in a discriminatory manner. One example for such manner could be a draft EO by POTUS that would give the US Department of Justice broad powers to prevent foreign adversaries like China from accessing Americans’ personal data.²¹⁸² This led to the understandable warning from Chinese Foreign Ministry spokesman Zhao Lijian that “while China believed each country had the right to take measures to protect the personal data and privacy of its citizens, relevant initiatives should be reasonable and scientific. They should not be relegated as a tool for individual countries to over-generalize the concept of national security, abuse national power, and unreasonably suppress specific countries and enterprises.”²¹⁸³

However, through an intervention such as we propose in this thesis, nations would no longer be “forced” to adopt competing regulations and declare that a country wishing to do business in its domestic market must have equivalent data protection laws, otherwise certain restrictions on the flow of data would apply. After all, since this intervention has to be designed to harmonize, the source of such behavior of nations, the fragmentation and disparity in data protection levels,²¹⁸⁴ should be remedied. Ultimately, it is important to avoid manifesting restrictions on TFPD in an intervention that would amount to “balkanization”; that is, subordinating regulatory measures to a strategy of digital protectionism, sometimes expressed as a response to “data imperialism”.²¹⁸⁵ The Commission also noted that it would like to address such restrictions through horizontal provisions that preclude such unjustified restrictions.²¹⁸⁶ Even if restrictions on the flow of certain types of personal data are permitted in an intervention for the reasons stated in this Section II.2, the rules from GATS²¹⁸⁷, by including the requirement of necessity, and that any measure taken with respect to the protection of personal data must not be a means of arbitrary or unjustifiable discrimination or a disguised restriction, could provide a safeguard to ensure that such restrictions do not go too far. GATS and GATT provide for the national security exception, while GATS also includes the “public order” exception. Therefore, a restriction on TFPD would be within the scope of GATS as an exception to the rule, based on “national security” and “public order” (law enforcement) grounds. To apply these exceptions, a “necessity test” is required, Art. XIV GATS. This test then would examine first whether the public policy objective is legitimate; this is to be assumed according to the above. Then, for the individual case, it would still have to

²¹⁸² Alper, A. [Alexandra] and Freifeld, K. [Karen]. (12 May 2022). Exclusive. Biden eyes new ways to bar China from scooping up U.S. data. *Reuters*. <https://www.reuters.com/world/us/exclusive-biden-eyes-new-ways-bar-china-scooping-up-us-data-2022-05-11>.

²¹⁸³ Alper, A. [Alexandra] and Freifeld, K. [Karen]. (12 May 2022). Exclusive. Biden eyes new ways to bar China from scooping up U.S. data. *Reuters*. <https://www.reuters.com/world/us/exclusive-biden-eyes-new-ways-bar-china-scooping-up-us-data-2022-05-11>.

²¹⁸⁴ Chapters II-VII

²¹⁸⁵ Von Arnould, A. [Andreas]. (2016). Freiheit und Regulierung in der Cyberwelt: Transnationaler Schutz der Privatsphäre aus Sicht des Völkerrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 1–34). C.F. Müller Verlag. P. 21.

²¹⁸⁶ Chapter II, Section II.4.5.; and Chapter IX, Section II.3

²¹⁸⁷ Chapter V, Section III.

be assessed whether this restriction, based on a specification of certain types of personal data to be included in the scope of this intervention,

- constitutes a means of arbitrary or unjustifiable discrimination; or
- is a disguised restriction on trade; or
- or imposes restrictions that are greater than necessary to achieve the objective.

In this way, horizontal provisions²¹⁸⁸, which have been increasingly used and are likewise measured against GATS, would have been incorporated into a solution. Concerns²¹⁸⁹ that the general objective of liberalizing transborder trade in services under GATS might conflict with the human-centric approach to personal data protection would also be addressed. In the event of a GATS-based challenge to the data protection framework embodied in an intervention, provisions restricting the TFPD would then not run such a significant risk of being rendered incompatible. UNCTAD noted that

the fact that the exceptions [also Art. XIV GATS] are loosely defined ultimately leaves it to these agreements' dispute settlement mechanisms to determine what is a "legitimate public policy objective" as a justification for restricting cross-border data flows. The same applies for the "necessity" provision: e.g. it "does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective". This would leave something as important as data regulations to be decided by panels of three experts, should member states bring about disputes.²¹⁹⁰

The design of this settlement mechanism is a subject of the operational objectives below²¹⁹¹.

3. Human-centricity

Atkinson / Cory correctly stated that

a central challenge is that many countries associate data governance with political and social control. Therefore, these countries will oppose global efforts to harmonize rules on data privacy (such as the EU's GDPR). Given the current values-based approach to global Internet policy, these countries are likely to be intractable in coming up with principles and mechanisms that allow robust encryption, privacy, and content moderation and related issues. Every nation needs to recognize that not every country it deals with on the global digital economy will share its values. This is a distinction that policymakers already acknowledge offline with traditional trade.²¹⁹²

Therefore, such "values" are to be integrated into an intervention, which as many countries as possible have in common with each other. Above²¹⁹³ it was found that "principles" and "essential guarantees" are present in certain frameworks and are based on a "human-centric" approach, which was stated above²¹⁹⁴ as an objective of the European framework, of the UN, and in parts also of China. An intervention should therefore include principles and essential guarantees recognized as extensive as

²¹⁸⁸ See Chapter II, Section II.4.5.

²¹⁸⁹ See Chapter VIII, Section I.1.

²¹⁹⁰ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 147.

²¹⁹¹ Chapter XII

²¹⁹² Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 226.

²¹⁹³ Chapter IX, Section III.2.; and Chapter IX, Section III.3.

²¹⁹⁴ Chapter IX, Section III.1.1.

possible recognized at global level, in particular in the mayor frameworks, the US, Europe, and China, to find consensus based on common goods as described above²¹⁹⁵. This also has the background that the European framework will probably not deviate far, if at all, from the self-imposed high level of protection, as Commissioner Vestager also noted, “because we take the guidance of course from the court [CJEU] who ruled on the basis of the Charter of fundamental rights which is not something that we can or will change. [...] we need to find a way of working with the Americans that is in accordance with this – in order of course not to get a negative *Schrems* III judgment, if so be.”²¹⁹⁶ The European frameworks’ essential guarantees would therefore most probably be the European minimum position for consensus. The essential guarantees described above²¹⁹⁷ therefore delimit the target field of this third specific objective.

The data protection principles set by the European framework are also recognized in ADPPA and PIPL.²¹⁹⁸ Although the data minimization principle is not present in the ASEAN framework,²¹⁹⁹ and the storage limitation principle not in the APEC framework,²²⁰⁰ an intervention should still include the seven principles common to the mayor three frameworks.

GDPR, ADPPA, and PIPL cover the first two²²⁰¹ of the four essential guarantees, although Chinese law shows partial weaknesses in the specification of its rules.²²⁰² The existence of the other two essential guarantees, “independent oversight mechanism” and “effective remedies to the individual”, are still disputable in both China and the US.

In China, remedies to the individual are regulated in the same way as in the European framework. However, since PIPL has only been effective for a relatively short time, it remains to be seen whether these remedies will also be applied “effective” and not only exist on paper. Two reasons could be cited against an “independent oversight mechanism” in China. First, the State has broad discretion in both legislation and enforcement through the passus “other duties and responsibilities provided in laws or administrative regulations” and “meeting any other requirements specified by the laws, regulations or the CAC”. Second, relevant departments of the State Council, and relevant departments of county-level and higher local governments, are called to perform protection duties according to related regulations; the responsibilities of these authorities among themselves – although PIPL now regulates those in Arts. 60-65 – are not as clearly limited as in the European framework.

If ADPPA would be adopted as proposed, the US framework would for the first time take a human-centric approach. Although the right to restrict processing and the right in relation to automated decision making and profiling are not explicitly mentioned in ADPPA, the analysis above²²⁰³ has found that both can be derived from the norm text. As also found above²²⁰⁴, there are still differences concerning the existence of an “independent oversight mechanism” and “effective remedies to the individual” to the European framework. The US has a longer way to go than China to align its level with the essential guarantees of the European legal framework. It remains to be seen whether

²¹⁹⁵ Chapter X, Section II.2.

²¹⁹⁶ Lomas, N. [Natasha]. (24 February 2022). *Privacy Shield 2.0 is high priority but not easy, warns EU's Vestager*. <https://techcrunch.com/2022/02/24/no-schrems-iii-pls>.

²¹⁹⁷ Chapter IX, Section III.3.

²¹⁹⁸ Chapter IX, Section III.2.

²¹⁹⁹ Chapter IX, Section III.2.

²²⁰⁰ Chapter IX, Section III.2.

²²⁰¹ Chapter IX, Section III.3.

²²⁰² which are: processing should be based on clear, precise and accessible rules; necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

²²⁰³ Chapter IX, Section III.3.

²²⁰⁴ Chapter IX, Section III.3.

the US legislature and/or the US executive branch will opt for a statutory or non-statutory solution, possibly even a mix of the two, and how this governance model would then mesh. In this regard, the details of the EU-US DPF remain to be seen. An independent “Data Protection Review Court” and an “Executive Order” to resolve problems of effective remedies for non-US citizens have been announced, but implementation effects in practice are yet unknown. Legal uncertainty also exists concerning a standing to bring an Administrative Procedure Act suit in federal court. It also remains to be seen with respect to the role of the FTC whether the latest financial aids will lead federal (and State SAs) to convergence with characteristics of SAs according to a European framework pattern.

Overall, both the US and China have taken significant steps toward alignment with the four essential guarantees of the European framework. This momentum should be used for specifying the content of an intervention at the international level. The third specific objective of this intervention must therefore be to adhere to the principles and essential guarantees of the European framework. This would also have the advantage that the Union could accede to this agreement through its personality under international law, as the contents of this agreement would not affect the GDPR or other provisions of Union law and would include an essentially equivalent level of protection. Any necessary deviations from this level could still be solved by means of trust and coordination; these are to be described below²²⁰⁵.

These essential guarantees should provide a legal means for data subjects to protect their rights, regardless of the place where infringements occur and the entity responsible for the violations. The essential guarantees should protect data subjects against unauthorized violations in both – as Rojszczak calls them – “horizontal” relationships (free from government interference) and “vertical” (free from interference from non-state actors) as well as against violations originating from legal entities operating from third countries and from third country authorities.²²⁰⁶ Also, the data subjects should be entitled to file complaints; this should not be available to States only (e.g. the so-called “inter-State complaints”, Art. 41 ICCPR). An intervention should also enable rights and obligations to arise directly from it. Data subjects should be able to claim their rights solely on the basis of the intervention. This would exclude an intervention that still needs transposition into national law.

In addition to the principles and essential guarantees, the question of which default position²²⁰⁷ should be included in an intervention is also relevant. It was found above²²⁰⁸ that none of the default positions has significant advantages or disadvantages but can be suitable depending on the nature of a national regulatory regime. Since no such position can be ruled out *per se* for an intervention, a solution of the most likely compromise (consensus) must be sought at this point. A default position essentially has three different approaches: First, the GDPR, which adheres to the prohibition principle. In the literature, especially from US sources, the focus lies still on the negative impact of the prohibition principle of the GDPR on the free flow of personal data and overall, on the development of the digital economy. This disregards that China regulates that only under one of seven conditions set out by Art. 13 PIPL, a controller may process personal data. Those conditions are alike those in the GDPR, except for Art. 13(7) PIPL. However, this similarity only concerns the first stage, not the second stage.²²⁰⁹ Concerning the

²²⁰⁵ Chapter X, Section II.5.; and Chapter X, Section II.6.

²²⁰⁶ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 26.

²²⁰⁷ Chapter IX, Section III.1.2.

²²⁰⁸ Chapter IX, Section III.1.2.

²²⁰⁹ Regarding the difference between “first stage” and “second stage” see Chapter II, Section II.3.1.

latter, China follows a more restrictive approach. Moreover, the rest of the frameworks generally allow data processing (first stage) and also TFPD (second stage), unless certain limitations apply. A third approach is the proposed ADPPA. It includes in Sec. 102 and Sec. 204 a prohibition principle for special types of personal data deemed sensitive, for the data processing activity as such; the second stage is not regulated in ADPPA, which could indicate that the same applies to the second stage. It seems to be the most preferable variant to regulate a prohibition principle in an intervention only for particularly sensitive data types. This should ensure that such data are particularly protected against the risks that the processing / transfer of such data may present for the interests, rights and fundamental freedoms of the data subject. “Special types of personal data” (although often named differently) are recognized in all the aforementioned frameworks²²¹⁰, which would facilitate consensus in this regard. Below²²¹¹, it will be determined in more detail which personal data fall under this “special” type. For all other cases, data processing (first stage) as well as a TFPD (second stage) should be allowed in principle. However, the principles for a legitimacy of such processing / transfer similar²²¹² to Art. 6(1) GDPR (first stage) and Art. 44 GDPR (second stage) should be observed. The inclusion of principles similar²²¹³ to Art. 44 GDPR is then also in line with the “conditional on safeguards” approach identified above²²¹⁴ as preferable. It was stated above that this approach should be deviated from in such a way that flow restrictions for the purposes of rational national security as well as public order are to be allowed within narrow limits²²¹⁵. The same must then also apply to cases in which a processing / transfer of personal data is generally prohibited, but exceptionally permitted based on these rationales.

One matter remained so far – regarding a possible intervention at international law level – not reflected in the literature. In the *Schrems* judgments, reference was made to a “measure in a democratic society”. GDPR and LED require “a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned”, Convention 108+ requires “provided for by law and such transfers constitute a necessary and proportionate measure in a democratic society”, the ECHR the legitimacy of an interference requires that, derived from the rule of law principle of the ECHR, that interference must be suitable, necessary, and appropriate, and the law which allows for an interference must be precise, and the EDPB “to make sure interferences with the rights to privacy and the protection of personal data, through surveillance measures, when transferring personal data, do not go beyond what is necessary and proportionate in a democratic society”. Not only from the objective of universality to be strived for, but also from the human-centric objective, it is questionable whether an intervention should refer so specifically to “democratic society”. We believe that this cannot be the case. An intervention should be guided by the UDHR. What constitutes a “democratic society” remained undefined in the UDHR. However, there is nothing wrong with referring to morality, public order, and the common good, as the UDHR does, and with requiring that the legitimacy of exceptions be subject to the rule of law and a proportionality test.

²²¹⁰ Chapters II-VI

²²¹¹ Chapter XII

²²¹² to be specified in more detail in Chapter XII

²²¹³ to be specified in more detail in Chapter XII

²²¹⁴ Chapter X, Section II.2.

²²¹⁵ to be specified in more detail in Chapter XII

4. Maturity

Another specific objective should be to reach the highest possible maturity level. An intervention should first regulate the current highest possible level and further improvement of this level should be integrated into such strategy²²¹⁶. If the level of maturity were defined too low in the intervention, the intervention would run the risk of not reaching the highest level in time in accordance with the strategy. If the level defined in the intervention were defined too high, there would be a risk that no consensus would be found. This fourth objective also includes points that cannot be clearly assigned to the other specific objectives of this Section II.

Above²²¹⁷ it was described that Europe has an advanced (GSMA classification) and comprehensive (de Terwangne classification) level. While the APAC framework is still progressive and self-regulatory in its entirety, China, as the most important Party to APAC, has progressed to an advanced/comprehensive level through its regulations since 2017, and it is expected that this will influence the level in APAC in the future. In the US, once ADPPA would be in place, an advanced level would also be established. However, ADPPA exempts the public sector from scope. Processing of personal data by federal government is governed primarily by two laws: the Privacy Act²²¹⁸ and the E-Government Act²²¹⁹. Separate laws in the US govern specific areas of the US public sector, such as the health-care system. Therefore, a comprehensive framework in the US cannot currently be assumed. Nevertheless, the objective of an intervention should be an intervention that also includes the public sector, to aim at universality²²²⁰.

The hypothesis of this thesis is that a binding regulatory instrument may be achieved. It has been found above²²²¹ that non-binding guidelines such as the OECD Guidelines or the UN Guidelines have not achieved the general objective of harmonization. Self-regulatory approaches such as Safe Harbor and Privacy Shield were criticized by the European side above all for their non-binding legal character. In addition to a binding character, however, an intervention would also have to be enforceable; these enforcement mechanisms will be described below²²²².

A pure self-regulatory and market-oriented approach in an intervention must be rejected for the intervention as such because of the deficiencies²²²³ associated to this approach. However, based on blended governance, elements of such an approach should complement the human-centric approach.²²²⁴

During the development of the intervention, the regulatory body should consult with all public and private stakeholders involved and engage with other data protection policymakers in other countries; this would then also be in line with the multi-stakeholder approach of this thesis. Prior to the adoption of the intervention, the regulatory body should adopt a data protection strategy that sets the timeline for achieving a data protection framework at the level of an advanced and comprehensive maturity. Planning, goalsetting and execution of such a strategy will be discussed below²²²⁵.

²²¹⁶ to be analyzed in more detail in Chapter XII

²²¹⁷ Chapter IX, Section III.1.5.

²²¹⁸ See Chapter III, Section II.1.1.1.

²²¹⁹ E-Government Act of 2002, Pub.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458

²²²⁰ See Chapter X, Section II.2.

²²²¹ Chapter V

²²²² Chapter XII

²²²³ See Chapter IX, Section III.1.1.

²²²⁴ See Chapter X, Section II.6.

²²²⁵ Chapter XII

5. Trust

A global ecosystem needs a global trust structure. To enable trustworthy transfers, a basis is required that minimizes risks and creates equal opportunities between the stakeholders. We agree with this basis as described by the WEF:

Openness, trust and interoperability today are conditioned on efficient cooperation where governments, businesses and users can effectively mitigate risks and ensure protection when data are transferred abroad. Such trust is often reciprocal by nature and arises more readily between legal entities that are prepared to abide by similar rules or offer equivalent levels of protection against risks. Jurisdictions that share similar legal concepts and offer effective enforcement and recourse to address any negative externalities arising from data flows between them, are more likely to share trust. Systems with deeper similarities – on constitutional order, ethical values or understanding of fundamental rights – are also less likely to diverge their rules in the future, even as new technologies emerge, or regulations are enacted.²²²⁶

The WEF included interoperability in their data governance approach, which will be discussed below²²²⁷. The WEF included two further necessary components of trust. On the one hand, technical measures, which also require technical development, i.e., should always be adapted to the state of the art;²²²⁸ on the other hand, it considered citizens and their trust as being crucial. The emerging data governance regime between government, companies and citizens has been particularly clearly differentiated in China²²²⁹ and it is to be expected that this division will not change quickly worldwide. Accordingly, the fifth specific objective of an intervention must be to ensure equal trust among all these three stakeholders.

From a government perspective, data governance is still associated with political and social control. This need for control is derived from various concerns. Emily Wu divided those into “technical concerns” and “value concerns” and correctly noted that the value concerns “are harder to articulate and harder to address”²²³⁰. This can be underlined by the significantly overlapping rationales identified above²²³¹.

The technical concerns are mainly related to the core problem discussed and should be addressed by an intervention with the results found above²²³²:

- Data flow restrictions do not improve data security; and
- data flow restrictions do not necessarily mean improvements for the domestic economy; and
- data flow restrictions are not the only way to ensure access for local law enforcement or regulatory supervision; and
- data flow restrictions do not remove the risk of foreign government access requests; and

²²²⁶ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 16.

²²²⁷ Chapter X, Section II.6.

²²²⁸ See Chapter X, Section II.7.

²²²⁹ Chapter VIII, Section II.

²²³⁰ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 17.

²²³¹ Chapter VIII

²²³² Chapter VIII, Section I. // See also Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 14–16.

- the cost of such data flow restriction policies can be hugely detrimental to the global economy.

An intervention should address such technical concerns by decreasing confusion, complexity, and those related misconceptions. Having such intervention in place for all stakeholders should then help alleviate the concerns that, e.g., data stored by dominating US “large data holders” (like the European definition of VLOPs) will be inaccessible to foreign governments in relevant to a criminal investigation. In general, trust needs to be strengthened that national law enforcement agencies can get access to domestic data stored in other nations. Therefore, law enforcement purposes within the “public order” rationale were also included above²²³³ as an exception to a prohibition on data flow restrictions. Law enforcement scenarios, however, do not only concern the penetration of foreign territories, but also other scenarios. Cory / Atkinson / Castro correctly stated that it is important “to recognize that not all data flows should be treated the same, as some data flows are rightly illegal”²²³⁴. They correctly argue that States should be allowed to block a flow of illegal data, as blocking of trade in endangered species or human trafficking is also supported in the “offline world”. However, legal checks and balances should be integrated to ensure an appropriate use of this possibility; also in order not to threaten the trust of the other stakeholders.

Value concerns are not just about restrictions of TFPD, but about the overarching category of national data sovereignty. These concerns are therefore also related to the others above in Chapter VIII, Sections II–III. One value concern is the fear of dependence on dominant US and Chinese providers. The EU articulated in its Data Strategy²²³⁵ that it is concerned about its ability to govern arising technologies according to its own rules and values, as it could be paralyzed by its dependence on these players and thereby relies mostly on the rationale of protecting the (supra)national digital economy. Therefore, even “the idea of neocolonialism [is] appropriate, as nations fear that by controlling access to technology, the U.S./China will have the power to control other key aspects of domestic life (such as the economy and even politics)”²²³⁶. The second value concern is a mistrust in foreign governments, in particular the access by foreign States to personal data of own citizens, as the NSA affair has made clear; similar, but vaguer, as not so comprehensively verified by whistleblowers, is this fear regarding China. The third value concern – again with Emily Wu – is the “fear of losing control”, which consists in the assumption that “without radically nationalist policies to govern the data of their citizens and handicap the growth of market competitors, they will lose control. Once their digital development is linked to the cooperation of foreign powers, they may be unable to regain independence and data sovereignty. Further, for countries like India, asserting independence against foreign colonial powers has been an integral part of the nation’s modern identity.”²²³⁷ To address such value concerns, an intervention should include a collaborative approach to technology innovation with all stakeholders. By allowing certain data flow restriction measures, sovereignty recognition could in principle be retained. At the same time, Member States should be obliged to use those measures only within certain limits, which are necessary and proportional and do not unduly affect other stakeholders. An intervention should include an explicit commitment to criticize neocolonialism with respect to data. This approach should reduce the perceived need for data localization laws in these less powerful countries. The use of data for innovation

²²³³ Chapter X, Section II.2.

²²³⁴ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²²³⁵ See Chapter II, Section II.3.8.2.

²²³⁶ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 17.

²²³⁷ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 17.

purposes should be enabled. It was mentioned above²²³⁸ that especially emerging technologies depend on amplifying a country's economic, informational and military power. To this end, an intervention should also include provisions similar to the aforementioned²²³⁹ "open data strategies". Although China, contrary to the European and US framework, does not yet have such a clear strategy, a consensus on "open data" should be easier in relation to other elements, as the WEF also noted: "Voices note that non-personal (and industrial) data is a critical input to the industry and involves less divisive policy issues, making a multilateral consensus more likely. Yet, the cross-border flow of non-personal data still depends on the granular details that govern the local definition of personal data since it is defined negatively, *e contrario*, as any data that is not personal information"²²⁴⁰.

Digitization requires trust in digital services and products for businesses to be successful. A more harmonized global approach could create more legal certainty for the global digital market from the perspective of businesses, which ultimately could build more trust from the customer side. Those responsible for TFPD therefore place trust close to the center of their interests. Open access to public data plays also a role for businesses. Here again, it becomes important to design an intervention as a bottom-up, multi-stakeholder initiative. Data collaborations should be set up to facilitate the public-private exchange of information, in addition to data sharing between businesses. An intervention should also "provide consumers with more control over their data as well as holding business accountable for their data practices. While this may be met with some resistance from industry, stricter regulation of the private sector could be ultimately beneficial for international business as it could reduce the fears that foreign nations have about the power of US tech companies"²²⁴¹. However, an intervention can only succeed if all public and private sector responsible for TFPD are equally obliged to comply with the binding intervention's obligations. Opening clauses similar to the GDPR²²⁴² should therefore be avoided in order not to create the risk that such clauses would create a competitive disadvantage for the responsible entities in such States that have not opted for the implementation of such clauses.

An intervention should also ensure that trust is established from the citizens' perspective. On the one hand, "chilling effects"²²⁴³ must be avoided by making the intervention clearer than the GDPR, especially in its scope. On the other hand, awareness and understanding by the general population must be brought about by ensuring that the intervention is "comprehensible to the average data subject, transparent in its nature and operation, and capable of effective regulation"²²⁴⁴. The aim of an intervention should therefore be to provide the citizen with sufficient knowledge of the effect of such intervention so that the citizen can then make an informed decision.

An intervention should ensure that its objectives are "S.M.A.R.T.", which means they should

be specific, measurable, achievable, relevant and time-bound. Specific objectives should be precise and concrete enough not to be open to varying interpretations by

²²³⁸ Chapter VIII, Section I.1.

²²³⁹ Chapter IX, Section III.1.5.

²²⁴⁰ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 16.

²²⁴¹ Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>. P. 19.

²²⁴² See Chapter IX, Section II.3.

²²⁴³ Chapter IX, Section II.3.

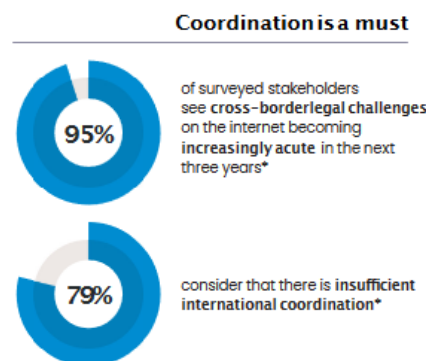
²²⁴⁴ Trakman, L. [Leon] and Walters, R. [Robert] and Zeller, B. [Bruno]. (2019). Is Privacy and Personal Data Set to Become the New Intellectual Property?. *International Review of Intellectual Property and Competition Law*, 937–970, <http://dx.doi.org/10.2139/ssrn.3448959>. P. 944.

different people. Objectives should define a desired future state in measurable terms, to allow verification of their achievement. Such objectives are either quantified or based on a combination of description and scoring scales. Policy aims should be set at a level which is ambitious but at the same time realistically achievable. The objectives should be directly linked to the problem and its root causes. Objectives should be related to a fixed date or precise time period to allow an evaluation of their achievement.²²⁴⁵

However, transparency should not be limited to the development of options for an intervention but be present in the whole regulatory process²²⁴⁶.

6. Cooperation

As the Internet & Jurisdiction Policy Network put it correctly, “cooperation is a must”.



Source: Internet & Jurisdiction Policy Network, “Infographic Internet Jurisdiction Policy Network”²²⁴⁷

However, it is important to delineate two areas of cooperation. On the one hand, those countries which would be directly covered by the scope of an intervention (“in-scope”), on the other hand, those which would not (“out-of-scope”). The WEF noted that “interoperability between each framework must be enhanced to allow data to flow more freely. [...] The notion of interoperability is also central since it can foster trust through all the pillars of the Osaka Track”²²⁴⁸. With the term “interoperability”²²⁴⁹, the WEF had in mind to develop elements of convergence between “different data protection systems”. Interoperability becomes relevant at the latest when transborder transfers between in-scope and out-of-scope countries take place. However, there are also elements which cannot be regulated by an intervention,²²⁵⁰ or which should not be covered by an intervention for reasons of a feared lack of consensus but should be cooperation-based. There are also elements that would affect both Member States and non-Member States of an intervention, and it is therefore necessary to distinguish when binding and/or cooperation-based would be appropriate. We therefore prefer to group the TFPD scenarios both inside and outside the intervention under “cooperation”.

²²⁴⁵ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 100–101.

²²⁴⁶ See Chapter XII, Section II.

²²⁴⁷ Internet & Jurisdiction Policy Network. (September 2020). *Infographic Internet Jurisdiction Policy Network September 2020*. <https://www.internetjurisdiction.net/uploads/pdfs/Infographic-Internet-Jurisdiction-Policy-Network-September-2020.pdf>

²²⁴⁸ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 7, 16.

²²⁴⁹ Defined in the “European Interoperability Framework” as the “ability of organizations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organizations, through the business processes they support, by means of the exchange of data between their ICT systems”. European Commission. (2023). *NIFO - National Interoperability Framework Observatory*. <https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/1-introduction#1.1>.

²²⁵⁰ For the peculiarities of building international uniform law see below Chapter XII, Section I.

It was stated above²²⁵¹ that an intervention should include the principles and essential guarantees of the European framework. If deviations of a substantive and/or temporary nature from these cannot be avoided, they should be resolved through cooperation. These deviations include, in particular, the essential guarantees “independent authority” and “effective remedies”, which still require development in both the US and China in order to reach the level intended by an intervention.

As explained above²²⁵², an intervention should also include those elements from the WEF’s data governance system that fall under “limited participation”. These elements are then to be included via cooperation and the blended governance model.

It is therefore worth considering whether subjects of international agreements could be covered, at least in part, by the intervention. One of these could be the MLATs. The goal should be, as Cory / Atkinson / Castro correctly suggested, “to establish and adopt model MLAT language, or a MLAT 2.0”.²²⁵³ This could prevent significant divergences between existing MLATs and enable “fairly standardized agreements across many nations”²²⁵⁴. To this end, an intervention should

create a common framework for when and how countries may use domestic authorizations to access data outside their borders. This may include arrangements such as reciprocal recognition of domestic search warrants (when countries meet certain legal standards) in order to expedite the process. Similarly, the agreement may include comity analyzes²²⁵⁵ or notice requirements as a condition of this reciprocal recognition. Second, MLAT 2.0 should commit countries to modernizing their methods for responding to foreign data requests. [...] Third, countries should commit to complying with their counterparts’ lawful requests for data in a timely fashion, unless those requests would violate mutually agreed upon provisions, such as for national security reasons. Fourth, countries should report the number of requests they receive, the number of requests they fulfill, response times, and progress in their modernization efforts. The goal of reporting is to hold participating nations publicly accountable for their timeliness in adopting and modernizing MLAT processes, as well as to identify inefficiencies in the process.²²⁵⁶

Care should also be taken to ensure that the intervention is consistent with other instruments of the same regulatory body. “Horizontal provisions, which were discussed above²²⁵⁷, as well as the trade agreements of limited participation described above²²⁵⁸, which are among the largest trade agreements besides the EU, must not contradict the subject of the intervention and GATS.

A top-down approach – as the European framework is called²²⁵⁹ – would ultimately not be able to address all differences in social, cultural, and political values, norms, and institutions behind countries. The GDPR, as shown above²²⁶⁰, has brought various flaws

²²⁵¹ Chapter X, Section II.3.

²²⁵² Chapter IX, Section III.1.4.

²²⁵³ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²²⁵⁴ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²²⁵⁵ See also Chapter III, Section II.1.2.7.; and Chapter VIII, Section III.

²²⁵⁶ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²²⁵⁷ Chapter II, Section II.4.5.

²²⁵⁸ Chapter IX, Section III.1.4.4.

²²⁵⁹ Exemplarily, see Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²²⁶⁰ Chapter IX, Section II.3

not only for the EU arena. These deficiencies should not be repeated in an intervention. Among them, the cooperation between SAs and a “one-stop-shop” mechanism should be more solid. It should also be avoided that SAs of the Member States of an intervention would jeopardize harmonization through divergent interpretations – as happened in the EU with the interpretation of the “sufficient supplementary measures”.²²⁶¹ For the EU, alternative models of enforcement of the GDPR, including a more centralized approach, have therefore been partially envisaged. There remains a question for Chapter XII as to how far enforcement of the intervention should be centralized. Not only should fragmentation be avoided with regard to the cooperation of SAs, but there should also be consistency of instruments within the scope of an intervention. The intervention should “address a series of challenges in order to enhance the protection of personal data”²²⁶², which the EDPB defined for 2021-2023.²²⁶³

With its Guidelines 2013, the OECD wanted to take the global dimension of the processing of personal data more into account and strive for global “interoperability”.²²⁶⁴ The data governance model of the intervention also needs to be “interoperable” (at this point not in the broader sense of a cooperation, but in the narrower sense). TFPD scenarios with external relationship should be conditioned on mechanisms and collaboration that build trust. Interoperability in this respect then means that

countries enact laws to address data privacy, cybersecurity, and other issues in broadly similar ways so that they each provides a similar level of protection or similarly addresses a shared objective, even if their specific legal and regulatory frameworks differ. At its most fundamental level, interoperability is the ability for firms to transfer and use data and other information across applications, systems, services, and jurisdictions. Interoperability is the most realistic goal for global data governance.²²⁶⁵

Non-UN States have also connection to the Internet and can use e.g. cloud computing, so out-of-scope countries can theoretically get in touch with personal data from in-scope States. Such non-UN States face the same challenges in applying their laws to MNEs. Interoperability based on the accountability principle would then not exclude the use of modern technology altogether but allow it under regulated conditions. These regulated conditions should create interoperability, especially since “interoperability is fighting to be the global consensus, as it is a mutually acceptable and beneficial principle to countries, regardless of their political system, their approach to data privacy, or level of development (as opposed to the disadvantages of harmonization and localization). Such an interoperable system would focus on global protections through local accountability.”²²⁶⁶ If trade agreements already exist or are to be concluded between States in-scope and States out-of-scope of an intervention, at least this minimum protection based on the accountability principle should be reflected in the subject matter of such agreements. Although a self-regulatory approach in-scope of an intervention must be rejected,²²⁶⁷ elements of such approach should be used – based on blended governance – for transfers to out-of-scope States and hereby complement the preferred

²²⁶¹ See Chapter IX, Section II.3.

²²⁶² EDPB. *EDPB Strategy 2021-2023*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_strategy2021-2023_en.pdf, (15 December 2020).

²²⁶³ See Chapter IX, Section II.3.

²²⁶⁴ OECD. (2023). *Privacy*. <https://www.oecd.org/digital/ieconomy/privacy.htm>.

²²⁶⁵ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

²²⁶⁶ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 227.

²²⁶⁷ Chapter IX, Section III.1.1.

human-centric approach for in-scope scenarios. A conceivable objective could also be to include terms of use or voluntary commitments tailored to specific areas of law or user groups. In the context of copyright or data protection law violations, the role of a SP should then be not to have to change too much in the direction of an arbitrator between data subjects. From the SP's point of view, there is a risk that, while meeting the demands articulated by one side, it will provoke criticism from others, which could lead to long-term controversy and ultimately hinder effective action. Therefore, if an SP guarantees government agencies to take effective action against certain content (e.g., hate speech), mechanisms should be established to ensure that only legitimate concerns get through. By means of economic incentives, an attempt could be made to influence the motivation of the stakeholders in such a way that when designing their services, they give preference to those variants that provide the individual fundamental rights in the least affect. Self-regulatory elements in an intervention should be guided by APEC's accountability-based CBPR. Those hold as the most important criterion for this section of the work that their standards are binding once a company has acquired membership. The advantage of CBPR is that they are effective for building trust between otherwise non-equivalent systems. Like the CBPR, interoperability is also at the heart of the OECD Guidelines. Also, one study had found that "84 percent of respondents stated they will apply for CBPR sometime within the next few years"²²⁶⁸, which would facilitate consensus.

For both in-scope scenarios and scenarios with external relationship, the multi-stakeholder approach mentioned above is necessary. First, because an intervention proposed in this thesis is also intrinsically dependent on intensifying dialogue to build trust for consensus, and second, for both in-scope scenarios and scenarios with external relationship, to promote a global culture of respect for personal data. For both, an intervention would need to engage in dialogue with all stakeholders involved in order to provide leadership in data protection and promote the highest possible harmonized level of protection worldwide. Interoperability also depends on such a multi-stakeholder approach which should develop common ways to mitigate risks and address shared concerns. An intervention should also promote supranational data protection initiatives in a certain region between out-of-scope countries to implement common principles for intervention and consider interoperability with the intervention. This would increase trust between in-scope and out-of-scope countries, facilitate the sharing of best practices among policymakers, and allow SAs to more easily detect and address non-compliance in scenarios with external relationship. This includes facilitating cooperation between SAs of Member States and such of out-of-scope countries, with a focus on cooperation in enforcement cases involving out-of-scope controllers/processors.

7. Innovation

An intervention should be able to keep pace with globalization and digitization. The convergence of international markets, the increasing influence of MNEs and the development of information and communications technology are just examples of the variety of challenges whose unforeseeable further developments should be manageable with an intervention.

These developments could lead to considerable friction (e.g., data fungibility vs. data minimization), which resulted in demands for a more modern data protection law.²²⁶⁹ The objective of an intervention should therefore be fit for the digital age and rethought,

²²⁶⁸ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²²⁶⁹ See also Chapter VIII, Section I.1.

namely from a potential “brake on innovation” to a “catalyst for innovation”. Gasser described the “forces at play”²²⁷⁰, and followed up his observations about the technological, economic, and behavioral forces by noting that the law, in factual response to the other forces, can functionally serve either as a constraint, enabler, or leveler. We agree with him that the law’s traditional function in response to digital technology has been a constraint, but that the law can “also serve the role of an enabler, where it opens up spaces for technological and social innovation and interaction, enables transactions, and supports various modes of production and collaboration. [...] The third basic function of law in the context of innovation is as a leveler. In this function, the law aims to correct a normative or market imbalance in power.”²²⁷¹ An intervention should avoid this “constraint” function and promote the other two. It should for example support the reduction of barriers to investment and bureaucracy, and the building of 21st century infrastructure in collaboration with stakeholders; goals that have been reflected in many regulatory measures since the turn of the century.

The challenges of globalization and digitization often lead to misconceptions of States. States are often overwhelmed with the “tension field” formed by “State interests” from their obligations and a “laissez-faire” global economic tendency. Some measures to restrict data flows have been enacted based on wrong assumptions. To eliminate these is also the general objective of an intervention. The Parties to an intervention – and the out-of-scope countries via cooperation²²⁷² – should be given a framework to prevent the tendencies of “data imperialism”. After all, it would be more difficult to reverse the effects of such tendencies at a later stage.

This should be avoided on the one hand by anticipatory regulation, and on the other hand by an evaluation cycle similar to the GDPR. This would require an intervention to “be agile and risk- and outcome-based, as domestic regulators and international cooperation will never keep pace with the rate of innovation. New technologies may also achieve better outcomes and compliance than sanctions-based models.”²²⁷³ Harmonization must therefore not lead to a “legal petrification of factual issues that must be kept open to political discussion because their solution depends on changing social and economic policy values”²²⁷⁴. The regulatory body should continue to study the challenges posed by new technologies and close gaps through an intervention. After all, a “failure to ensure continued data flows would result in missed innovations, economic gains and societal advances. Governments will impose irreparable losses on citizen welfare and industrial competitiveness if they adopt disproportionate restrictions.”²²⁷⁵ Attention should always be paid to the overall goal of a free flow of data, not only for the initial intervention, but also for its adjustments based on this evaluation cycle.

Flaws from the European framework²²⁷⁶ should be avoided. Like the European market, the market of the global digital economy requires a constant regulatory process to meet the objectives of improvement. Future digitization will be influenced by the intervention. Improvements through the intervention must therefore be continuously measured against the needs of digitization. Risk neutrality in the intervention would pose a risk, as

²²⁷⁰ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 355–374. // See also Chapter I, Section I.

²²⁷¹ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 368–369.

²²⁷² See Chapter X, Section II.6.

²²⁷³ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 12.

²²⁷⁴ Kötz, Hein, “Rechtsvereinheitlichung – Nutzen, Kosten, Methoden, Ziele”, in: Rabels Zeitschrift für ausländisches und internationales Privatrecht, Mohr Siebeck, Vol. 50 (1986), Iss. 1, pp. 1-18 [p. 12]

²²⁷⁵ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 17.

²²⁷⁶ See Chapter IX, Section II.3.

it would then not be possible to react appropriately to new technologies such as AI, which are leading to an increasing “asymmetry of power between large data-processing companies and the people whose data are processed”.²²⁷⁷ Care should be taken to ensure that the accountability principle, which would have to be included in the intervention,²²⁷⁸ does not lead to obligations of those responsible for the processing of personal data that would be inappropriate on the basis of the risk-based approach. The prohibition principle of the GDPR should be limited to specific data types (e.g., sensitive personal data).²²⁷⁹ In this respect, one of the main criticisms of the GDPR could be resolved, namely that it may inhibit innovation.

Agility and risk-based also mean that technological developments that are already known should be included in the intervention. This applies, for example, to AI. In this regard, Atkinson / Cory stated that

many nations and regions, especially Europe, are pushing for a regime of global AI regulation, rightly understanding that not all AI systems will comport with EU values or laws. And while global efforts to develop and implement AI governance principles (such as that AI systems should minimize undesirable AI bias) are useful and warranted, going further and codifying these into some kind of international legal agreements would be not only difficult to do, but also likely harmful to innovation.²²⁸⁰

By referring to “undesirable AI bias”, Atkinson / Cory suggested what was outlined above as a solution: First, to exclude certain effects of new technologies from a free flow of data through data flow restrictions for certain data types (e.g., sensitive personal data), and second, to limit restrictive measures by ensuring that they do not harm innovation too much; regarding the latter, WTO core principles of non-discrimination, most-favored-nation treatment, and transparency would come into play in a limiting way.²²⁸¹ This way of limiting the threat of new technologies to citizens is lived out in the offline world. Agreeing with Atkinson / Cory, States should “have the same right to do the same with digital products, including ones with AI in them”²²⁸². Including those principles in an intervention should help “ensure countries can address legitimate public policy objectives, but in a way that ensures that domestic regulation is not used as a de facto trade barrier”²²⁸³.

Digitization is also accompanied by the development of digital content. For an intervention with the specific objective of promoting innovation, it is therefore important not to prevent such content, but to promote it as a catalyst. This promotion is confronted with obstacles that must be considered for an intervention. Atkinson / Cory wrote appropriately that it is

critical to recognize that countries can have conflicting rules and regulations regarding values-related digital content (in terms of how each country determines what is and is

²²⁷⁷ Roßnagel, Alexander / Geminn, Christian, “Datenschutz-Grundverordnung verbessern”, *Nomos*, 2020, p. 153

²²⁷⁸ However, not as the sole data transfer mechanism, since it was found above that the “conditional on safeguards” transfer is preferable. Nevertheless, as in the GDPR, accountability remains an underlying principle.

²²⁷⁹ See Chapter X, Section II.2.

²²⁸⁰ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). *Cross-Border Data Policy: Opportunities and Challenges*. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 228.

²²⁸¹ See Chapter V, Section III.

²²⁸² Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). *Cross-Border Data Policy: Opportunities and Challenges*. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 228.

²²⁸³ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). *Cross-Border Data Policy: Opportunities and Challenges*. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 228.

not illegal online). Countries that are realistic about the task of building a broad rules-based global digital economy need to accept (even if they do not necessarily like) the fact that some countries censor information on the Internet for political and social purposes.²²⁸⁴

In the EU-US arena, for example, this is also related to the fact that the EU does not have as strong a commitment to free speech as the US. Above²²⁸⁵, it was already noted that determining “universal bads” as well as “universal goods”, has a positive impact on the consensus-building for an intervention. However, digital content creation is so diverse and dependent on all four dimensions mentioned above²²⁸⁶, that universalism is difficult in this respect. We therefore agree with Atkinson / Cory, who found policymakers and advocates also need to recognize that the practice of authoritarian nations to limit access to certain websites and web pages does not constitute the breaking of the internet” and that “it is important to recognize that not all data flows should be treated the same, as some data flows are rightly illegal. For example, over 30 countries (including many democratic, rule-of-law countries) use website blocking to prevent access to websites engaged in large-scale copyright infringement, illegal gambling services, financial fraud, and child pornography”.²²⁸⁷ However, we find that limits on data flow restrictions should be observed by the GATS rules, just as law enforcement activities should be supported by cooperation.

In addition to preparing for new technologies, however, such technologies could also be used at the time of enactment of an intervention. As to be analyzed in detail below²²⁸⁸, the use of new technologies alone is not sufficient to achieve the objectives. However, new technologies are needed in a supportive way. Either a specific intervention using individual technology or a technology-neutral one can be considered. In principle, if a technology poses too many risks or legal problems and therefore needs to be regulated by a new instrument, a legislator should create a specific standardization for it; if it does not pose too many risks or legal problems, the legislator should instead adopt a technology-neutral regulatory instrument. In our case, this means that, where legal rules seek to prescribe a certain technology, they may prevent useful innovation or they may, if not developed within a certain timeframe, become meaningless due to the accelerating technological development. Such rules may also represent an additional cost factor which might be unduly burdensome at least for some stakeholders involved. Therefore, the protection of data subjects should be technology-neutral and not depend on the techniques used to avoid a serious risk of circumvention of the rules. In practice, there are major deviations and uncertainties in the technical implementation of data protection measures. This problem should be addressed in advance in an intervention by issuing technical guidelines for implementation. At the same time, the intervention should offer an opportunity for legal science and technology to jointly develop standards. Examples are the consent to data processing according to Art. 1(1a) GDPR as well as the exercise of data subject rights according to Arts. 15ff. GDPR. In an intervention, for example²²⁸⁹, the principle of “one-in-one-out” (or also “global opt out”)²²⁹⁰, should be introduced to minimize the burdens for citizens and companies by paying special attention to the

²²⁸⁴ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 228–229.

²²⁸⁵ Chapter X, Section I.

²²⁸⁶ Chapter I, Section I.

²²⁸⁷ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 229.

²²⁸⁸ Chapter XI

²²⁸⁹ Other operational objectives will be discussed in Chapter XII

²²⁹⁰ “global opt out” is already carried out promisingly by Californian law, which introduced the “Global Privacy Control (GPC)”, to communicate a Do Not Sell request required under the CCPA. See also <https://globalprivacycontrol.org/>

impact and costs of implementing the legislation – especially for SMEs.²²⁹¹ As found above²²⁹², data security is an important part of a regulatory framework when data security can support the protection of personal data. Data security measures therefore play an important role in the principles of various frameworks.²²⁹³ Data security measures should therefore also be included in the intervention and coordinated with data protection measures. This includes encryption as a measure. Encryption has become a fundamental component of improving cybersecurity for all stakeholders. Cory / Atkinson / Castro rightly stated that “any government attempt to undermine encryption reduces the overall security of law-abiding citizens and businesses, makes it more difficult for companies from countries with weakened encryption to compete in global markets, and limits advancements in information security”.²²⁹⁴ An intervention should declare at least an intention on investments in data security measures that are recognized as fundamental (the evaluation cycle and the multi stakeholder approach should help to determine this) to the success of the digital economy. Effective protection of data subjects should also be supported by providing suitable infrastructures to services. Regarding information technology, one could particularly think of services that provide trustworthy communication or secure storage of data. The obstacle to governmental services is often the lack of acceptance, as users sometimes place less trust in State infrastructures than private companies, for example.

Legal, technological, market-based, and legal approaches should work together. This also includes, as the WEF stated, that, “given the open nature of the internet and the global trading system, governments must also leave room for alternative mechanisms (like the certification of trusted businesses) when intergovernmental cooperation cannot provide an immediate solution”²²⁹⁵. A way of fulfilling a State’s obligations is to control the SPs and their products on the market by means of certification or accreditation. In this way, fundamental rights holders are given the opportunity to use services that are classified as trustworthy. For the SPs there is the possibility to have the fulfillment of pre-determined statutory minimum requirements confirmed and to prove this with a quality mark, such as e.g., the initiative of “E-Mail made in Germany”²²⁹⁶. Such a seal of approval can be of importance since data subjects often cannot oversee all technical processes behind services. The advantage of such accreditation concepts is that data subjects are provided with national or supranational trustworthy services that are also subject to these legal frameworks and the respective enforcement measures.

Interoperability “improves regulatory outcomes and trust as jurisdictions with similar legal concepts and approaches address issues that arise from cross-border data flows similarly”.²²⁹⁷ Interoperability can foster innovation, competition, and consumer choice by facilitating access and development of more data and data-driven services, which reduces barriers to market entry.²²⁹⁸ Therefore, attention to the specific objective of “cooperation” is also important for an innovation-promoting intervention. For example,

²²⁹¹ European Commission. *Better Regulation – joining forces to make better laws*, COM(2021)219, (2021). P. 1.

²²⁹² Chapter I, Section II.5.4.

²²⁹³ Chapter IX, Section III.2.

²²⁹⁴ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²²⁹⁵ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 16.

²²⁹⁶ <https://www.e-mail-made-in-germany.de/>

²²⁹⁷ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

²²⁹⁸ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

the intervention should consistently observe the UN's Sustainable Development Goals (SDGs)²²⁹⁹ to ensure that the intervention contributes to sustainable development.

III. Conflict of objectives

An intervention must be justified and must not cause conflicts of objectives. The Commission also noted that – which is also the case in this thesis – “when objectives are multiple and interrelated, it is important to highlight the links between them, particularly any possible trade-offs”²³⁰⁰. Hence, “when we aim at providing safety and security for a society which has human rights at its core, we must do so in a way that promotes human dignity. Living in a dignified society is not possible without the right to privacy – regardless of how safe or unsafe it might be. In conclusion, what we need is both: Privacy AND Security”²³⁰¹. An intervention is already justified

if one of the following conditions holds: (i) Further policy effort for liberalization and facilitation is required. (ii) Market failure due to the existence of externalities, the existence of public goods, economies of scale, imperfect competition, or incomplete/asymmetric information is found, and a policy to correct or cancel out market distortion can be effective. (iii) Important values or social concerns other than economic efficiency such as privacy protection, public morals, human health, or national security exist. (iv) Policies are needed in order to accommodate data flows and new data-related businesses [...].²³⁰²

Among these, the condition of a market failure was the most difficult to assess. Drexl also noted that “the extent to which the protection of personal data can be incorporated into a market-based analysis, for example in the sense of a market failure doctrine or in the context of an antitrust assessment, is by no means clear”²³⁰³. Following the analysis above, in particular in Chapter VIII, it can be noted at this point that all of the above conditions (i - iv) actually apply to the current state of regulation.

In the aforementioned list of conditions, it is striking that both purely economic and other considerations play a role; the latter can be in contradiction to a purely economic view. Drexl mentioned first and foremost the human-centric tension between freedom of information and the protection of life and health; the former ideally leads to complete and non-discriminatory access to all content on the Internet in accordance with the principle of net neutrality, while the latter ensures protection from security-related services, especially of the IoT, which actually speaks against the principle of net neutrality.²³⁰⁴ Furthermore, he noted that current technological developments are leading to new security policy problems.²³⁰⁵ Fukunari wrote in his comments on a framework proposed by the T20 that “if privacy is to be rigorously protected as a human right, as is argued in

²²⁹⁹ UN. (2023). *The 17 goals*. <https://sdgs.un.org/goals>.

²³⁰⁰ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 66.

²³⁰¹ Gstrein, O. [Oskar]. (28 May 2018). *Surveillance, Security, Privacy: What direction to reach the end of the tunnel?*. <https://www.juwiss.de/51-2018>.

²³⁰² Chen, L. [Lurong] et al. (29 March 2019). *The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies*. <https://t20japan.org/policy-brief-digital-economy-economic-development>. P. 4.

²³⁰³ Drexl, J. [Josef]. (2016). Regulierung der Cyberwelt – Aus dem Blickwinkel des internationalen Wirtschaftsrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 95–158). C.F. Müller Verlag. P. 127.

²³⁰⁴ Drexl, J. [Josef]. (2016). Regulierung der Cyberwelt – Aus dem Blickwinkel des internationalen Wirtschaftsrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 95–158). C.F. Müller Verlag. P. 127.

²³⁰⁵ Drexl, J. [Josef]. (2016). Regulierung der Cyberwelt – Aus dem Blickwinkel des internationalen Wirtschaftsrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 95–158). C.F. Müller Verlag. P. 127.

Europe, regulation may become more and more strict, undermining economic efficiency. Meanwhile, when it comes to the matter of national security, as in the case of the debate on cybersecurity, the policy debate goes nowhere beyond the preservation of security, with the issue of social welfare excluded from consideration”.²³⁰⁶ Iakovleva summarized that “on the one hand, the EU Charter of Fundamental Rights (EU Charter) guarantees the protection of the rights to privacy and the protection of personal data as fundamental rights. On the other hand, in its external trade policy the EU seeks to liberalize cross-border data flows and to maintain and further develop a globally binding rules-based trading system that ensures appropriate access to foreign markets for EU businesses”.²³⁰⁷ An intervention should ensure, as contained in the “data free flow with trust” initiative of former Japanese prime minister Shinzo Abe, that “openness and trust exist in symbiosis, not as contradictions”.²³⁰⁸

This shows the three main fields between which a conflict of objectives is possible: human-centric vs. economy-centric vs. security-centric, and, underlying all these fields, openness vs. trust. From a methodological point of view, we agree with Drexl, who noted in this respect that

the economic assessment should always form the starting point of the analysis. The starting point is therefore the question of whether government intervention is necessary to enable economic activity on the Internet in the first place or to respond appropriately to cases of market failure. This assessment is first and foremost suited to bring rationality into many discussions on current regulatory issues. It may also show that other policy goals can already be adequately pursued via an economic assessment. Only if this is not the case it is necessary to weigh the economic assessment against conflicting objectives.²³⁰⁹

Steinrötter described the aim “to improve the commercialization of data, and above all to promote data trading required for big-data applications” as “data economic law”.²³¹⁰ Although this term is concentrated on “non-personal data and/or even data as such, meaning the syntactic level”²³¹¹, his considerations also apply to this thesis. He noted that “whereas restrictions on the free movement of data (such as certain requirements imposed by public authorities on the location of data for storage or processing purposes) could constrain the development of the data economy, a data economic law potentially supports the free flow of data”, as “data protection law cannot counteract innovative considerations in particular relating to exclusive rights or access concepts *a priori*”.²³¹²

The perspectives of data economic law and data protection law can therefore clash. This must be balanced because both, as also the OECD noted, naturally generate interactions: “While regulations related to privacy and security are not traditionally

²³⁰⁶ Fukunari, K. [Kimura]. (7 January 2020). *Developing a policy regime to support the free flow of data: A proposal by the T20 Task Force on Trade, Investment and Globalization*. <https://cepr.org/voxeu/columns/developing-policy-regime-support-free-flow-data-proposal-t20-task-force-trade>.

²³⁰⁷ Iakovleva, S. [Svetlana]. (2021). *Governing cross-border data flows: Reconciling EU data protection and international trade law*. [Doctoral thesis, Faculty of Law, Universiteit van Amsterdam (I. Venzke)]. <https://hdl.handle.net/11245.1/cf54d2a9-cd41-42c2-94f1-24c81f8a3abd>. P. 311.

²³⁰⁸ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

²³⁰⁹ Drexl, J. [Josef]. (2016). Regulierung der Cyberwelt – Aus dem Blickwinkel des internationalen Wirtschaftsrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 95–158). C.F. Müller Verlag. P. 127.

²³¹⁰ Steinrötter, B. [Björn]. (2020). Legal Framework for Commercialisation of Digital Data. In M. [Martin] Ebers and S. [Susana] Navas (eds.), *Algorithms and Law* (pp. 269–298). Cambridge University Press. P. 272.

²³¹¹ Steinrötter, B. [Björn]. (2020). Legal Framework for Commercialisation of Digital Data. In M. [Martin] Ebers and S. [Susana] Navas (eds.), *Algorithms and Law* (pp. 269–298). Cambridge University Press. P. 272.

²³¹² Steinrötter, B. [Björn]. (2020). Legal Framework for Commercialisation of Digital Data. In M. [Martin] Ebers and S. [Susana] Navas (eds.), *Algorithms and Law* (pp. 269–298). Cambridge University Press. P. 272–273.

associated with trade, they can have trade consequences, when, for instance, they affect the movement of data that is critical for the coordination of global value chains or for a SME to trade.”²³¹³ National strategies, by their very nature, often overlook the fact that international trade and human rights are even more related to international security as a result of globalization. Security itself is an important common good, but not the most important one, because it is bound to other values such as human freedom, human dignity and the protection of the environment. In case of conflict, both economic and security objectives must therefore be subordinated to the objectives of a protection of fundamental rights. The only exception to this is the specific objective of universality analyzed above²³¹⁴. It was found that restrictions of specific objectives other than universality should be made possible as long as the rationale “national security / public order / sovereignty” is concerned. Legal goals such as informational self-determination will only be guaranteed by States in a global network if they enable their citizens to use globally effective technical tools. In parallel, however, the States must maintain their function to facilitate this. Without a functioning State, the fulfillment of its negative and positive obligations²³¹⁵ towards its citizens would be disturbed. Thus, attention must be paid to the most essential interests of States in “national security / public order / sovereignty”. Otherwise, as mentioned above²³¹⁶, a consensus between a State and other States would be more difficult, which would ultimately lead to an intervention not being realized at all. Through this weighing of interests we think that these conflicts of objectives identified in this Chapter X could be resolved.

IV. Conclusive remarks

UNCTAD has stated that

the diversity of views and dimensions on the key characteristics of data and cross-border data flows, and the associated complexities, points to the need for careful assessment of all elements involved when designing policies. Since different factors can play in different directions, different interconnections and interests involved need to be accounted for. The combination of the different issues [...] may lead to multiple combinations of policies that will require policy choices to be made, according to political and societal decisions, and on the basis of development objectives. Overall, there is no simple solution.²³¹⁷

The objective of our proposed instrument needs to – with Naef –

combine a commitment to the free flow of personal data across borders with high data protection standards and therefore offer a new avenue for data protection without data protectionism. [...] Restrictions on cross-border flows of personal data oriented toward protecting fundamental rights – such as laid out in EU data protection law – comply with international trade law and thus should not be interpreted as protectionist when applied consistently. This is clear from the fact that restrictions oriented toward protecting fundamental rights would disappear if third countries implemented stronger uniform data protection legislation and followed international human rights law pertaining to surveillance practices.²³¹⁸

²³¹³ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Para. 3.

²³¹⁴ Chapter X, Section II.2.

²³¹⁵ See Chapter IX, Section I.2.1.

²³¹⁶ Chapter X, Section II.1.

²³¹⁷ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 93.

²³¹⁸ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 425, 439.

We have made our “policy choice” with the general objective (Chapter X Section I). An intervention harmonizing the existing rules is needed, which by its binding effect addresses legitimate concerns raised by TFPD, while supporting the free flow of data as a general principle.

Chapter X Section II followed up on the “elements” of a framework analyzed in Chapter IX. It was found that the first specific objective must be to harmonize the exogenous variables²³¹⁹ based on consensus among the endogenous variables²³²⁰.

In the case of the other specific objectives in Chapter X Section II, it is noticeable that they “oscillate” between hard law components and soft law components.²³²¹ Both sides are indispensable for the intervention and follow the blended governance approach of this thesis. Important for a distinction between hard law and soft law components is whether a TFPD scenario takes place between States in scope of the intervention (in-scope States), between in-scope States and out-of-scope States, or between out-of-scope States. Within the intervention, the rules would be harmonized, mature and human-centric; in this regard, mainly hard law components are applied. The more a TFPD turns to a scenario with external relationship, the more the solution consists of soft law components. The latter applies in particular to the specific objective of cooperation, and therein to interoperability. Weber / Staiger prefer a “hybrid” approach, which we only follow in parts for the necessary non-legislative elements. But Weber / Staiger found correctly that

at least a partial societal consensus on privacy norms must be reached. This consensus on pre-legal norms then enters the legal system and interacts with the existing legal norms. In this context, learning mechanisms are essential in order to bridge the gap between the values of society, the regulatory norms in place, and technological developments. Norms must be designed in a manner that allows implementing a plurality of regulatory modes and tools.²³²²

In developing the objectives, care was taken to integrate the main advantages of the three most important frameworks for the global digital economy – US, Europe, China – into the intervention; elements of the WTO rules were also used. This is in line with the multi-stakeholder approach of this thesis. From the European framework would need to be used that the intervention should be binding and human-centric. Otherwise, no consensus could be reached with the EU, which, due to its high level of data protection, is fundamentally unable “to genuinely engage and collaborate with counterparts unless its privacy preferences prevail over everyone’s else”²³²³. As a transfer mechanism, the “conditional on safeguards” approach accessible to firms of all sizes and not only sector-specific should be used, as this allows the greatest possible flexibility. However, several derogations are necessary to allow countries such as China under certain conditions to protect legitimate interests. The general scope of transfer mechanism should allow restrictions for certain data types under conditions based on the rationale of “national security / public order / sovereignty”. However, such a legitimate public policy objective would then have to submit to the necessity test from Art. XIV GATS. The intervention should include all principles and essential guarantees of the European framework. In fact, a main advantage from China is a well thought-out and consistent system on a level almost as high as that of the European framework. Although based on strong economic

²³¹⁹ See Chapter IX, Section III.

²³²⁰ See Chapter IX, Section I.

²³²¹ See also Chapter I, Section II.5.5.

²³²² Weber, R. [Rolf] and Staiger, D. [Dominic]. (2017). *Transatlantic Data Protection in Practice*. Springer. P. 137.

²³²³ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

expansion interests, China has recognized that it needs a mixture of a fixation of principles and essential guarantees on the one hand, but on the other hand a – also from our point of view – necessary recognition that specific data types need specific rules. The US framework shows that a default position of a prohibition of data processing in the European frameworks' nature is not tenable for an intervention but must be limited to specific data types (especially sensitive personal data). Also, self-regulatory mechanisms are helpful for scenarios with external relationship because of the market-oriented tradition in US data protection law, as the US is a signatory in important international trade agreements. Another point that should not be taken from the European framework and others is to refer specifically to “democratic society”; we believe it is better to refer to morality, public order, and the common good, as the UDHR does. The intervention should regulate as high a maturity level as possible, which is advanced (GSMA classification) and comprehensive (de Terwangne classification); because all three frameworks important to the global digital economy (the US at enactment of ADPPA) also reach this level.

Up to this point, we have mostly turned to the hard law components in the concluding remarks. We disagree partly with Cory / Atkinson / Castro when they stated that “it is unrealistic and impractical to demand universal rules on privacy. A better option would be to create an interoperable, accountability-based system that works for all countries and the various ways they enact data privacy and protection.”²³²⁴ We have shown that while universality may be achievable, a mere voluntary accountability approach for TFPD scenarios with external relationship would not lead to the full achievement of the general objective. However, we agree with some recommendations of Cory / Atkinson / Castro, which are assigned to soft law. Especially the specific objectives of trust, cooperation and innovation have shown us that an intervention without soft law components would not be feasible.

An intervention should restore trust in the system of international trade. It should encourage stakeholders to improve transparency about how personal data are processed, including at the global level. To do so, however, the intervention must address various technical concerns and value concerns by reducing confusion, complexity, and related misunderstandings, particularly about the impact of data flow restrictions. It should be designed to be collaborative and include multistakeholder forums and intergovernmental forums in the development of the intervention as a trust-building measure. By allowing certain data flow restriction measures, the intervention also addresses a major value concern from a State perspective, the potential loss of sovereignty. From a business perspective, the intervention should establish trust in digital services and products; this will require a harmonized global approach to create more legal certainty for the global digital market. The citizens (data subjects) perspective must also be addressed by ensuring awareness and understanding among the general population that the intervention is understandable to them, transparent in its nature and operation, and capable of effective regulation. For all stakeholders, all objectives of the intervention must be specific, measurable, achievable, relevant, and time-bound.

The principle of cooperation also applies to the relationship of the intervention with out-of-scope States. A preferable approach of the GDPR, despite the problems associated with its extraterritorial reach, should be integrated, namely to set a “gold standard”;²³²⁵ the gold standard then no longer being the GDPR, but the intervention. The intervention can then still “form the foundation for broader debate, adaption, and adoption to expand

²³²⁴ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

²³²⁵ See Chapter IX, Section II.3.

more issues and countries”²³²⁶, but from a position of strong, harmonized hard law. The intervention should support out-of-scope States (especially developing countries in capacity building) to help them build their data governance frameworks and advocate for transparency and good regulatory practices as part of trade agreements. However, to protect trade between in-scope States, the intervention should provide legitimate countermeasures against out-of-scope States that adopt measures to restrict the flow of personal data. Interoperability is an important principle to be established by the intervention; exemplified by the fact that the intervention should consistently adhere to the UN’s Sustainable Development Goals (SDG). Such improvements should be enabled also ex-post through an evaluation cycle similar to the one of the GDPR.

The intervention should be committed to be innovation-promoting. The GDPR has also adopted various innovative elements which, following the blended governance approach, complete what is in principle a pure rules-based solution with further elements. This approach is to be followed in principle. Nevertheless, the intervention should avoid flaws from the European framework and thus take advantage of the fact that in the course of the last four years since the effectiveness of the GDPR, some problems of the GDPR have been identified that can potentially inhibit innovation. Technology innovation is to be considered both *ex-ante* and *ex-post* of a regulation by the intervention. The intervention should include a collaborative approach to technology innovation with all stakeholders and at the time of its enactment use new technologies, e.g., measures for data security and such facilitating data subjects’ consent. The intervention should be agile and risk- and outcome-based, as well as technology-neutral. Certification measures should also be allowed. Accordingly, in an intervention SPs should be given the opportunity to be audited and certified against national and international standards. This would also help to increasingly include regional infrastructures (especially those for providing cloud services) in the scope of the intervention.

Chapter X has also established that an intervention would be justified in itself, that conflicts of objectives potentially exist but could be resolved by weighing of interests. However, an international legal instrument should only be sought at all if the objectives of such an intervention cannot be sufficiently realized by the nation States (so-called “efficiency test”) but can be better realized at the international level because of their scope and effect (so-called “added value test”). Within the European framework, a “subsidiarity principle”, that is, whether the Union should act, exists in Art. 5(3) TEU and is applied here by analogy. However, it was disputed in the EU for some time whether self-regulation or co-regulation initiatives were also included in this principle. This was first clarified by the “Better Lawmaking” agreement²³²⁷, which states that “the three Institutions recall the Community’s obligation to legislate only where it is necessary, in accordance with the Protocol on the application of the principles of subsidiarity and proportionality. They recognize the need to use, in suitable cases or where the Treaty does not specifically require the use of a legal instrument, alternative regulation mechanisms.” To fulfill this proportionality, a weighing of interests is to be conducted, which consists, as noted above in this Section III, primarily of an economic assessment. It should therefore also not be possible to fulfill the same policy objective in a way that has a less restrictive effect on trade; this position was also taken by the OECD, stating that

²³²⁶ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

²³²⁷ European Parliament, European Council, European Commission. (31 December 2003). *Interinstitutional agreement on better law-making*, OJ C 321. P. 1–5.

it is important to bear in mind the underlying goals of the government. As for all policy-making, it is important to consider how effective the measures are in achieving their stated aims, the associated costs and trade-offs, and whether there are alternative measures that would enable a better balance among different aims to maximize overall benefits for the population. From a trade policy perspective, of interest is whether the same policy objective can be fulfilled in a way that has a less restrictive effect on trade.²³²⁸

The considerations on “subsidiarity” are based on the findings from Chapters II to VIII that the existing regulations show differences and lead to problems. This fragmented legal framework worldwide inadequately protects the fundamental rights of data subjects as their personal data are increasingly processed transborder. The existing patchwork of national rules is also a significant obstacle to the free exchange of goods and services, as those responsible for such TFPD face additional costs and administrative burdens. Nation States cannot sufficiently achieve the objectives set forth in this Chapter X. If the rights of data subjects are not to be played off against each other in the jungle of national regulations, it is better to regulate data protection uniformly at the international level. In addition, the international legal framework promises greater clout vis-à-vis MNEs as a further added value.

²³²⁸ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Para. 17.

CHAPTER XI: OPTIONS FOR INTERVENTION

Corresponding with the specific methodology²³²⁹ of this thesis, the aim of this Chapter XI is “to consider as many realistic alternatives as possible and then narrow them down to the most relevant ones for further analysis”²³³⁰. In proceeding further in this Chapter, we follow the Commission, which defined four steps:

- (1) Construct a baseline from which the impacts of the policy options will be assessed;
- (2) Start by compiling a wide range of alternative policy options;
- (3) Identify the most viable options; explain the discarded policy options;
- (4) Describe in reasonable detail the key aspects of the retained policy options to allow an in-depth analysis of the associated impacts.²³³¹

The baseline is “the benchmark against which the impact of the policy options is compared”²³³² and includes all relevant national, supranational, and international regulations that are assumed to remain in force; we have presented these in Chapters II - VII. For the present Chapter, steps (2)-(4) of the Commission therefore remain to be discussed. The baseline should also “include expected socio-economic developments (ageing, GDP growth, etc.) as well as important technological, market and societal developments, such as the pervasive nature of the internet, social media, and emerging technologies, which by themselves are causing large changes and challenges”²³³³; we have presented these in Chapter I. Options for intervention “should be closely linked to the drivers of the problems, the problems themselves and the identified objectives”²³³⁴; we presented problem drivers, problems, and objectives in Chapters VIII and X. The aim of this Chapter is to identify as many policy responses as possible within the context of policy constraints and possible room for maneuver. To be considered are also the options for which the stakeholders identified above in Chapter IX would likely provide support, based on their interests examined there. This Chapter XI should allow for the exclusion of options that clearly do not address those problems or objectives. It should also then be possible to identify the most viable policy instrument to achieve the objectives. Policy responses should be classified in the course of this Chapter according to whether they are less intrusive or more interventionist, and whether they are more classical instruments or suggested by more recent developments.

²³²⁹ See Chapter I, Section II.4.

²³³⁰ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 112.

²³³¹ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 112.

²³³² European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 112.

²³³³ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 112.

²³³⁴ European Commission. *Better regulation toolbox - November 2021 edition*.

https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 112.

I. No action

A “no action” option would mean not proactively addressing existing problems. This would follow the market economy idea that self-regulation is better than sovereign intervention. Not even self-regulatory “measures” would come into consideration, because this would already mean regulatory intervention in the current situation, albeit of a non-legislative and thus less intrusive nature. It must therefore be asked whether the situation could theoretically improve by itself, as such improvement of the current situation is inevitable according to what has been established so far in thesis.

In its strongest form, a “no action” option could be equivalent to a “post-privacy” movement. In Germany in particular, a standpoint had formed that no longer viewed data protection as positive, but as partially backward, unrealistic and undesirable. Post-privacy representatives²³³⁵ believed that a new social interaction is necessary to deal with this situation and that it shouldn't be technically prevented that freedom of information arises on the Internet. Although this would mean that data protection would no longer be enforceable, which would affect many individuals, technology should – from their point of view – adapt, not the individual. Post-privacy can therefore be seen as a counter thesis to the approach of a regulation of data protection.

The underlying idea that data protection has become obsolete also occurred in the US – for example with Mark Zuckerberg²³³⁶ – but there was no organized movement. The term “post privacy” was first used around 2009 in connection with a debate about social networks, which included the question, whether data protection should continue or whether, given the large amount of personal data on the Internet and its ease of distribution, data protection should be abandoned. During the debate about Google Street View in spring 2010,²³³⁷ parts of the German public expressed for the first time that data protection in Germany may actually be viewed too strictly. At the same time, WikiLeaks made the first classified documents public.²³³⁸ This loss of control was nevertheless largely received positively. These events scratched the previously unreservedly positive image of data protection.

Post-privacy, however, remains a utopia. An increasing number of individuals are inhibited by the fear of too much publicity and live in corresponding social constraints, in which a disclosure of personal data would be significantly dangerous to them. This is particularly prevalent in States with a longer tradition of privacy, such as in Germany. That is why former German Federal Minister of Justice Leutheusser-Schnarrenberger also argued against the post-privacy theory and considered it to be fundamentally wrong and dangerous.²³³⁹ In her view, personal data are not an abstract quantity, but the digital capture of a human individual. She also commented that post-privacy gives the wrong answers to the challenges of the increasingly networked world, because it is based on indifference and thus intellectual surrender. She argued that the gathering of personal

²³³⁵ Reißmann, O. [Ole]. (10 March 2011). Privatsphäre ist so was von Eighties. *Der Spiegel*. <https://www.spiegel.de/netzwelt/netzpolitik/internet-exhibitionisten-spackeria-privatsphaere-ist-sowas-von-eighties-a-749831.html>. // ctrl+verlust, (23 March 2011). *Was ist Postprivacy (für mich)?*. <https://www.ctrl-verlust.net/was-ist-postprivacy-fur-mich>.

²³³⁶ Kirkpatrick, M. [Marshall]. (10 January 2021). *Facebook's Zuckerberg Says The Age of Privacy Is Over*. The New York Times. <https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html>.

²³³⁷ Gathmann, F. [Florian]. (10 August 2010). Google überrumpelt urlaubende Ministerinnen. *Der Spiegel*. <https://www.spiegel.de/politik/deutschland/street-view-start-google-ueberrumpelt-urlaubende-ministerinnen-a-711073.html>.

²³³⁸ Wikileaks. (2023). *WikiLeaks Reveals Secret Files on All Guantánamo Prisoners*. <https://wikileaks.org/gitmo>.

²³³⁹ Leutheusser-Schnarrenberger, S. [Sabine] et al. (27 October 2011). Wir sollten nach der Ohrfeige einen Schritt zurücktreten. *Frankfurter Allgemeine Zeitung*. <https://www.faz.net/aktuell/feuilleton/debatten/staatstrojaner/sabine-leutheusser-schnarrenberger-im-gespraech-wir-sollten-nach-der-ohrfeige-einen-schritt-zuruecktreten-11508374.html>.

data by MNEs (in particular VLOPs) and States, the creation of user profiles and the collection of the sensitive personal data would result in a concentrated transborder power, democratically legitimized control would become increasingly difficult; therefore, greater sensitivity in handling personal data is necessary. According to Leutheusser-Schnarrenberger, the discussion about an Internet charter cannot be limited to purely legal questions, the digital world therefore not only needs new laws, but universal values ensured by self-regulation and alternative solutions.

The objective of a free flow of data (including personal data) is found in all frameworks examined above. With Directive 95/46 and the GDPR, the objective of the protection of personal data has become an integral part of economic activity, whilst the latter is to be supported by a flow of personal data as free as possible. Ensuring freedom of information – even in its most comprehensive form of access to all content on the Internet in accordance with the principle of net neutrality – while at the same time protecting personal data is not a contradiction, both objectives are not mutually exclusive.²³⁴⁰

Nevertheless, this free flow should take place based on applicable rules on data protection. A disembodied social space has formed on the Internet, in which almost all activities that are possible in the physical world are realized in a disembodied way. This also includes the many familiar problems of social coexistence. In order for legal transactions supporting social coexistence to become a reality on the widest possible scale, regulations are needed that enable trust and legal certainty in a world in which people meet only virtually. With a “no action” option, national and supranational laws are likely to evolve in an uncoordinated way, leading to an even greater patchwork of different levels of data protection. Problem drivers and problems are then also likely to evolve, worsening the situation. Without action, there would be no possibility to influence the problem drivers²³⁴¹, neither could behaviors be influenced in a manner that would address the problems²³⁴², nor concerns expressed by stakeholders²³⁴³ be addressed or policy objectives²³⁴⁴ be achieved. The “mapping stage”²³⁴⁵ – as the Commission calls it during a RIA – can thus identify “no action” as an option which is to be discarded.

Since the current situation of TFPD needs an order, the question arises whether it must be an own order that specifically applies to this situation. In this thesis, many peculiarities of this legal field have been presented so far, which leads us to the conclusion that the old legal rules for the offline world do not fit anymore. Those offer neither effective protection nor sufficient legal certainty, do not provide a framework for new developments, and prevent many online use cases by being tied to place, time, or physicality. Whether a separate legal system is necessary for the necessary problem-adequate rules, whether these should be formulated in separate laws or integrated into existing ones, and which type of legal measures could be used for this purpose, will be discussed in Sections II and III of this Chapter. The question then arises whether these rules must be made by democratically established law. Alternatives are self-regulation by the addressees of the regulations and regulations incorporated in technology.

²³⁴⁰ See Chapter X, Section III.

²³⁴¹ See Chapter VIII

²³⁴² See Chapter VIII

²³⁴³ See Chapter IX, Section I.

²³⁴⁴ See Chapter X

²³⁴⁵ European Commission. *Commission Staff Working Document, Impact Assessment, Accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118 final, (17 April 2018). P. 41.

II. Non-legislative action

This Section II groups all non-legislative actions. These are less intrusive than legislative actions. Non-legislative actions can also be combined with legislative actions.

There are numerous self-regulation tendencies within the global ecosystem of TFPD, which are divided into pure self-regulation, regulated self-regulation and co-regulation.²³⁴⁶ Those have in theory the potential to harmonize data protection rules across borders. Regulated self-regulation brings almost the same advantages as pure self-regulation but also offers some protection of State interests, which normally characterizes legislative action. Co-regulation actually belongs to the side of legislative measures, because in such measures a legislative measure delegates the realization of the objectives set by the legislative authority to non-governmental partners recognized in the field. Co-regulation shall nevertheless already be dealt with here because of its connection to self-regulation. Co-regulation could use the advantages of pure self-regulation and regulated self-regulation and counteract the respective disadvantages as far as possible. If provisions within a co-regulatory approach are created which meet the characteristics of clear and specify rules, conformity with them could lead to a rebuttable presumption of compliance with binding provisions.

It is important to what extent non-legislative action would be suitable for effectively addressing the problems and objectives analyzed in this thesis. Non-legislative action could maintain the trust of data subjects in the protection of their personal rights in a business area of high heterogeneity and dynamism, e.g., by developing – together with all stakeholders – models of technical data protection and compensation for unavoidable consequences for data subjects. By its nature, non-legislative action also corresponds to a multi-stakeholder setting in a blended governance approach, which requires for a regulatory culture in which regulation and self-regulation are not in competition. Weber / Staiger commented that

a hybrid approach to regulating data protection currently presents the best way forward, as it takes the need for clear rules as well as the technological capabilities of various industries into account by enabling them to create their own technological and organizational data protection frameworks that are based on the applicable industry characteristics. [...] A common argument brought by industry professionals is that the law does not suffice in taking into account the practical needs of the online industry and the law-maker's lack of technical knowledge. Furthermore, the path dependency inherent in the law-making process, as well as the enforceability of laws in the international context, raise questions as to the effectiveness of the laws and their ability to adjust to market conditions. [...] Enshrining privacy enhancing technologies and privacy by design in the normative framework is a good example of the law setting a basic requirement to take privacy into account in the design of a product or service whilst leaving enough leeway to enterprises to decide how to best implement privacy.²³⁴⁷

We agree that non-legislative measures can usually be made more flexible than it is the case with binding rules. This flexibility could then facilitate to react faster to technical progress, but also to special local conditions and their change. Non-legislative action could therefore also correspond to cultural particularities of an area in data protection issues. This could gradually approximate different local data protection rules.

²³⁴⁶ See Chapter VI

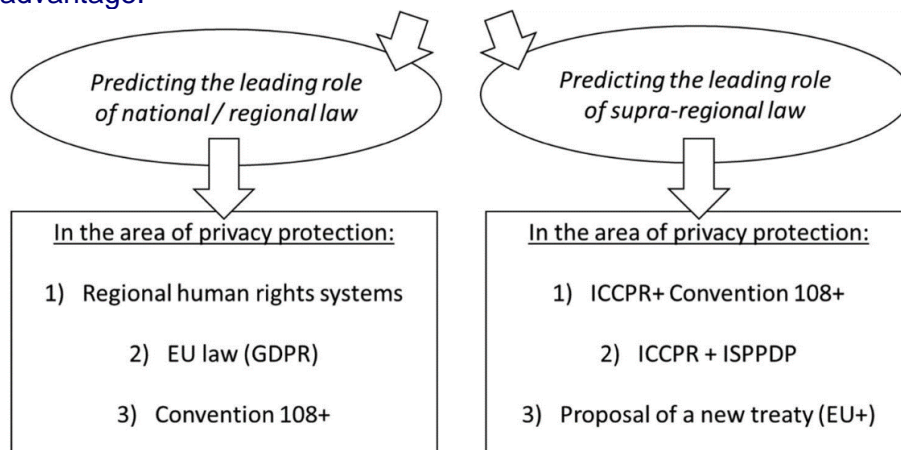
²³⁴⁷ Weber, R. [Rolf] and Staiger, D. [Dominic]. (2017). *Transatlantic Data Protection in Practice*. Springer. P. 135–137.

Nevertheless, the problem that is still inherently attached to non-legislative action remains: it creates non-binding rules and usually leads to a lack of acceptance and enforcement. It is also unlikely that there will be a general use of such rules; rather, only a part of the private sector worldwide would subject themselves to those, which would endanger universality. Even with explicit self-regulation by most companies, uncertainty would remain as to how potential competitors will behave in data protection matters. This could lead to a disadvantage of the participating companies on the market compared to those who do not submit to those rules. Moreover, a willingness of participants in the global digital economy to cooperate beyond national borders is crucial for a non-legislative action, since the powers of public authorities are in principle limited to the territory of their respective State. Such participants may find the requirements less practical and not sufficiently problem oriented. It is not uncommon for such participants trying to avoid or counteract legislative actions by forum shopping; they might be tempted to do the same with non-legislative actions. Cooperation in the private sector could be increased if rules were co-regulated with these addressees, be created in a more flexible nature, and be kept up to date with state-of-the-art technology.

A pure non-legislative action in an intervention would not outweigh the deficiencies associated to this approach. While non-legislative measures in the field of technical data protection are fundamentally promising, without the addition of any binding regulation it would prove to be an insufficient answer to the problems and objectives. Based on blended governance, non-legislative elements should nevertheless complement legislative action, especially for TFPD scenarios with external relationship.

III. Legislative action

Legislative action can take place through the improvement of existing regulation or through enactment of new regulation. To this end, before analyzing national, supranational, and international²³⁴⁸ options below²³⁴⁹, we want to refer to Rojszczak's²³⁵⁰ approach. We agree with him that, when exploring options, it is important to consider how "two general and, at the same time, opposing concepts of the regulation can be used to advantage.



Source: Rojszczak, M. [Marcin], "General approaches to regulating cyberspace in legal systems"²³⁵¹

²³⁴⁸ Whereby Rojszczak uses the term "supra-regional". We understand his term – according to the hierarchy of norms of international law – for the purpose of this thesis as synonymous with "international law".

²³⁴⁹ Chapter XI, Section III.1.1.; and Chapter XI, Section III.1.2.

²³⁵⁰ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44.

²³⁵¹ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 36.

The first one assumes that the primary source of regulation should be national and supranational laws, whereas supra-regional norms of international law should be used only as supplementation, especially for the determination of the relevant jurisdiction (choice of law clauses). [...] The second concept presumes the leading role of international legal regulations. Some extreme advocates of this approach have proposed the establishment of cyberspace as an autonomous area of jurisdiction.²³⁵²

Both multi-stakeholder and blended governance approaches used in this thesis are helpful in this respect and can be assigned neither exclusively bottom-up nor top-down. On the bottom-up side, all stakeholders must be involved in order to ensure the flow of information to the central body. On the top-down side, goals are set centrally, but, as described above²³⁵³, the smaller units must be involved in order to subject critical fields to a further cross-check and, in particular, to support trust and cooperation. Blended governance is helpful in ensuring that information is drawn from as many sources as is useful for the objectives and that a correspondingly large number of resources are used for the recommended measures to mitigate the risk.

1. Improvement of existing regulation

Improvement includes the approximation of legal systems through common principles. Improvement is a natural goal of every legislator. In view of the large number of stakeholders involved and the decreasing relevance of borders on the Internet, it is a challenge to identify the most viable normative level for standardization. As a rule, not only one level is affected, and all three levels could legitimately be assumed to have a normative interest.

1.1. National / supranational law

If legislative action is required for TFPD, the next question is whether this should lead to a globally uniform legal order. In principle, there is no objection to a regulation being made at the level closest to the citizen. In principle, this would then be national law. The Internet creates a uniform “cyberspace” for electronic economic and legal transactions, for which the most uniform rules possible should be established. If we want to promote the information society, economic growth, and investment in innovation by means of a free flow of data, then it seems necessary, based on what has been said so far, to subject the activities of the stakeholders in the global ecosystem of TFPD to a harmonized legal system. Returning to Rojszczak’s approach, this system could, however, theoretically also be created bottom-up. In this respect, there are two ways to choose from: the unification of the substantive law or the approximation through conflict of laws rules.

For every transborder data flow, conflict of laws rules would determine which country’s national law regime applied. However, there is not (yet) a specific conflict of laws rule for data protection. Classic conflict of laws rules reach their conceptual limits when there is not only a selective overlap of legal regimes to be dealt with but when one legal regime structurally spills over into the other, or when a ubiquitous technical phenomenon – such as the Internet – is involved. Among other things, this raises the questions of whether the principles of sovereignty and its delimitation can be transferred to the scope of this thesis, which State has regulatory sovereignty, which has the right to intervene, whether the territory could be used as a genuine link or would this lead to arbitrary results in

²³⁵² Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 36–37.

²³⁵³ Chapter X

cyberspace, whether the availability of Internet content in one country is sufficient or whether cumulative aspects must apply, and how this all relates to the principle of “*lex loci solutionis*”, which the EU sees as the connecting factor.

Laws with extraterritorial reach can lead to conflicts with the sovereignty of other States. In a system based on territoriality, extraterritorial regulations also affect the interests of other States. These interests need not necessarily relate to a State’s own territory but can also affect legal transborder matters. A limitation of this effect is therefore necessary to avoid conflicts, the permissible scope of an extraterritorial regulation should hereby be observed. So far it has been largely unclear if and under what conditions national data protection laws could be expanded to extraterritorial circumstances.²³⁵⁴ To date, there is no international convention which covers the allocation of regulatory sovereignty in international data protection law.²³⁵⁵ In the absence of such conditions, the “genuine link” requirement and the connecting factors should be used in data protection law.²³⁵⁶

This raises the question of the extraterritorial effect of human rights. The UN HRC argued that the Parties are required to respect and to ensure the rights of the ICCPR

to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party. [...] This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained.²³⁵⁷

The ECtHR maintained that “sovereignty” bound under Art. 1 ECHR exists in principle only on the territory of the Member States, and that extraterritorial binding on human rights is therefore the exception.²³⁵⁸ The ECtHR also relied on the criterion of “authority and control over individuals” in addition to territorial control.²³⁵⁹ In this respect the question arises whether and when surveillance of foreign Internet communication, as an example of TFPD scenarios, is comparable to have “control over individuals”. The Internet relies on infrastructure and data which are stored on servers that have a physical location, whilst data flows go through fiber optic cables. However, relying solely on forms of physical contact could lead to rather random results. A web server for example can be in a State that has no connection to the sender and recipient of a message; in addition, a relocation to another server is possible at any time, especially in cloud computing environments. The infrastructure alone as a connecting factor is therefore misleading. Technological progress largely makes physical domination of a place or a person unnecessary. Models depending on a territorial or personal connection are insufficient for TFPD scenarios, as the Internet not only enables unlimited virtual communication but also unlimited virtual access to the same communication.

The solution could be a *functional approach*, as the Maltese judge Bonello called for in the *Al-Skeini* judgment.²³⁶⁰ The distinction between positive and negative obligations for

²³⁵⁴ Svantesson, D. J. B. [Dan Jerker B.]. (2013). *Extraterritoriality in Data Privacy Law*. Ex Tuto Publishing. P. 19 f.

²³⁵⁵ Svantesson, D. J. B. [Dan Jerker B.]. (2013). *Extraterritoriality in Data Privacy Law*. Ex Tuto Publishing. P. 19 f.

²³⁵⁶ See Chapter VIII, Section III.

²³⁵⁷ UN, HRC. *General Comment No. 31 (80). The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add.13, (26 May 2004). Para. 10.

²³⁵⁸ ECtHR, Judgment of 7 July 2011, *Al-Skeini and others v. The United Kingdom*, Application no. 55721/07. Para. 74

²³⁵⁹ ECtHR, Judgment of 7 July 2011, *Al-Skeini and others v. The United Kingdom*, Application no. 55721/07. Paras. 133 ff.

²³⁶⁰ ECtHR, Judgment of 7 July 2011, *Al-Skeini and others v. The United Kingdom*, Application no. 55721/07. Paras. 78 ff.

a State is hereby of importance. Human rights are deemed to be defense rights without a particular “jurisdictional link”. Wherever the State can intervene in human rights, it justifies its sovereignty simply by exercising this ability. The implementation of human rights’ protective obligations ends nevertheless at the sovereignty of other States. Still, the State remains obliged to take appropriate action to ensure that third Parties do not violate the right to data protection of individuals in territories under its control. When concretizing a right to data protection at the global level, it remains necessary to differentiate also between public and private as well as between domestic and foreign stakeholders²³⁶¹. While common approaches to data protection law for public stakeholders can still be effective, other approaches must eventually be pursued for private stakeholders. For foreign stakeholders, the question of being bound to and the enforcement of national data protection regulations arises.

In its defensive dimension, the right to data protection has its grounds in the ECtHR jurisprudence on State surveillance.²³⁶² The practice of the UN HRC also followed the ECtHR judiciary.²³⁶³ State surveillance measures must serve an admissible purpose and be proportionate. Ensuring public security can be such a legitimate purpose.²³⁶⁴ However, there are concerns about the extent of such purpose. The UN Special Rapporteur for freedom of expression argued against misuse, especially in surveillance contexts, and proposed the narrowing of this legitimate purpose.²³⁶⁵ A group of NGOs and human rights lawyers encouraged that interferences with the right to data protection should only be carried out to protect “outstandingly important common goods” that are necessary in a democratic society.²³⁶⁶ A UN report provided arguments regarding the proportionality of those surveillance measures: mass surveillance programs such as “Prism” or “Tempora” make surveillance the rule, they reverse the relationship between rule and exception between freedom and restriction - and for this reason alone are inadmissible, even if they pursue legitimate goals. A blanket obligation for private individuals to data retention is also disproportionate.²³⁶⁷ The report also criticized the blurring of limits between enforcement agencies, intelligence agencies and other State bodies.²³⁶⁸

The State also has a duty to protect its citizens from unjustified interference with their personal self-development, be it through the exercise of its own sovereignty or through third States. In this dimension, a States regularly has a wide scope for decision-making, particularly in foreign policy. If the violations are carried out by the authorities of other States, the sovereignty of that other State limits the possibilities for reaction. Nevertheless, the respective State of the violated citizen(s) can then react by diplomatic

²³⁶¹ See also above Chapter IX, Section I.

²³⁶² ECtHR, Judgment of 1 October 2008, *Liberty and others v. The United Kingdom*, Application no. 58243/00. // ECtHR, Judgment of 18 August 2010, *Kennedy v. The United Kingdom*, Application no. 26839/05.

²³⁶³ UN, HRC. *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation*, <https://www.refworld.org/docid/453883f922.html>, (8 April 1988). Para. 4. // UN, HRC. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*, (30 June 2014). Para. 28: “authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.”

²³⁶⁴ CJEU. Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland v Seitlinger and Others*, C-293/12, ECLI:EU:C:2014:238. Para. 42.

²³⁶⁵ UN, General Assembly. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40*, (17 April 2013). Paras. 57 ff.

²³⁶⁶ EFF. (10 July 2013). *International Principles on the Application of Human Rights to Communications Surveillance*. <https://www.eff.org/files/necessaryandproportionatefinal.pdf>.

²³⁶⁷ UN, HRC. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*, (30 June 2014). Para. 26

²³⁶⁸ UN, HRC. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*, (30 June 2014). Para. 27

means or, if applicable, an interstate complaint to the UN HRC or the ECtHR. If there is a violation of the law, countermeasures can also be used to avert the violation; indirectly, this would also serve to protect the rights of data subjects.

States should also have a regulatory obligation regarding data processing by private stakeholders. This has largely been clarified for the domestic context. A UN Report demanded that States should clearly express expectations towards their domestic enterprises that human rights standards should be respected.²³⁶⁹ The UN Resolution on privacy in the digital age called for States and others to adapt their national legislation also to international human rights obligations regarding third-party violations.²³⁷⁰ What the content of those commitments in national law would be is still the question. Where and as long as a human rights protection obligation does not yet act as a lever, best practices could therefore be agreed. Those could encompass the legal figure of “due diligence” as a flexible concept, which is influenced by new knowledge and standards and is thus open to interpretation in the light of non-binding norms.

However, a State’s duty to protect for foreign activities of domestic companies is not yet fully established in international law. The UN HRC interpreted Art. 2(1) ICCPR that the term “ensure”, read with the rest of the Covenant,

requires States Parties to protect against violations by both State agents and private persons or entities. The obligation is one of means rather than result - States Parties should act with due diligence to take appropriate steps to prevent, punish, investigate and redress harm by private entities. The HRC indicates that the duty to protect applies to all rights so far as they are amenable to application between private persons or entities. However, it also appears that the Committee will assess the specific nature of this duty depending on the right in question, especially where the Covenant expressly states that a particular right should be protected by law.²³⁷¹

Art. 17 ICCPR takes limited account of the main protection of the positive dimension in its Section 1 by not exposing anyone “to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation” and derives from this in Section 2 a duty to protect: “Everyone has the right to the protection of the law against such interference or attacks.”

The extraterritorial reach of not fundamental but sub-fundamental, respectively simple national data protection laws, is also questionable. The fact that EU data protection law has extraterritorial effects is not due to an expansion of the EU’s claim to regulation itself, but rather due to technical developments. The prescriptive jurisdiction was based on Art. 4(1)(a) Directive 95/46 and the *Google Spain* case – now it is based on Art. 3 GDPR.²³⁷² The CJEU does not claim extraterritorial jurisdiction to enforce for the Union; rather, it merely enforces the conditions of access to the EU internal market. Anyone wishing to offer Internet services in the EU must comply with the data protection regulations applicable within the Union.

²³⁶⁹ UN, HRC. *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, A/HRC/17/31*, (21 March 2011). Para. 2: “to promote, secure the fulfilment of, respect, ensure respect of and protect human rights”.

²³⁷⁰ UN, HRC. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37*, (30 June 2014). Para. 4b

²³⁷¹ UN, Office of the High Commissioner for Human Rights. *State Responsibilities to Regulate and Adjudicate Corporate Activities under the United Nations’ core Human Rights Treaties*, <https://media.business-humanrights.org/media/documents/files/reports-and-materials/Ruggie-ICCPR-Jun-2007.pdf>, (June 2007). P. 4.

²³⁷² See Chapter II, Section II.3.1.

Where international law guarantees a right to access the market (e.g., within the framework of the WTO), an enforcement of a State's data protection provisions may be justified if it would maintain the principle of proportionality.²³⁷³ A differentiation according to the content of the respective data processing activity is then necessary. Svantesson found in this respect that "it is simply not productive of good results to view the question of extraterritorial claims from the perspective of whether they should be allowed or not in relation to data privacy laws. Indeed, it is not sufficient to ask when such claims are justified in relation to data privacy laws." He proposed to "introduce a more sophisticated delineation of the extraterritorial scope of such laws" and distinguished three "layers": abuse-prevention layer, rights layer; administrative layer.²³⁷⁴ When determining proportionality, it must also be considered that a data controller can assign its activities to different legal systems. The search for a proportionate balance between its right to access the market and the requirements of data protection can therefore also lead to practical concordance between competing jurisdictions in TFPD scenarios.

Antitrust law could also help reduce the power of global players on the Internet. Companies such as Microsoft, Amazon, Google and Meta have become so successful that they have largely taken over their respective markets. The market dominance of these companies is attributed to their efficiency, the peculiarities of bilateral markets, and the power that comes from controlling huge amounts of data. Personal data can strengthen a company's market power, while dominant companies can in turn collect larger amounts of personal data. It is therefore not surprising that digital markets and especially their market leaders have caught the attention of regulators. Regarding dominant companies, the question arises of what is to be understood as an abuse of market power in markets where the consumer does not pay a cash price. A free online platform model, which provides strong incentives for collecting personal data, has links to exploitative conducts under competition law. Collecting personal data could be an abuse in the form of an inflated price or in the form of unfair terms and conditions. If excessive data collection is classified as a case of imposing unreasonable prices, it must be assumed that data can be assigned a quantifiable price, which in turn is difficult to determine.²³⁷⁵ Even China, despite its protective approach to national digital economy, had responded to the strong market power of some companies and fined a domestic company, Alibaba, USD 2.8 billion after an antitrust investigation. In its decision of 6 February 2019²³⁷⁶, the German Federal Cartel Office (BKartA) prohibited Facebook from making use dependent on the processing of their off-Facebook data in its General Terms of Use. In addition, Facebook was prohibited from processing the off-Facebook data without the consent of the users on the basis of the General Terms of Use applicable at the time. The BKartA based its decision on the fact that the processing of personal data of the platform's users as provided for in the General Terms of Use constitutes an abuse of Facebook's dominant position in the market for online social networks for private users. In particular, the processing of off-Facebook data cannot be reconciled with the values underlying the GDPR, according to the BKartA. This raised the question of what the aim and mandate of antitrust law should be with regard to online platforms. In digital markets, it is becoming increasingly difficult to unravel the competition and data protection mandate areas. A key reason for this is that consumers in digital markets often do not pay the services in cash price. Instead, they receive services in exchange for their data. This means that the consumer damage resulting from market power is manifested in these markets as data protection damage rather than in the form of higher prices. Data protection law regulates the processing of data by all companies operating on the market.

²³⁷³ Art. XIV c) ii) GATS

²³⁷⁴ Svantesson, D. J. B. [Dan Jerker B.]. (2013). A "layered approach" to the extraterritoriality of data privacy laws. *International Data Privacy Law*, 3(4), 278–286. P. 280, 286.

²³⁷⁵ Regarding "data ownership" see above Chapter VIII, Section II.

²³⁷⁶ German Federal Cartel Office (BKartA), Judgment of 6 February 2019, B6-22/16. Paras. 573-870

It is not unusual for antitrust law to target regulated markets. With regard to the collection of data, antitrust law provides for additional obligations for dominant companies in addition to data protection law. In practice, it may not always be clear which of these two enforcement tools should take precedence. The CJEU Advocate General Athanasios Rantos noted in this respect that

while a competition authority does not have jurisdiction to rule on an infringement of the GDPR, it may nevertheless, in the exercise of its own powers, take account of the compatibility of a commercial practice with the GDPR. In that respect, the Advocate General emphasizes that the compliance or non-compliance of that conduct with the provisions of the GDPR may, in the light of all the circumstances of the case, be an important indication of whether that conduct amounts to a breach of competition rules.²³⁷⁷

The new FTC chairwoman, Lina Khan, confirmed hereto a “rowing recognition that persistent commercial data collection implicates competition as well as privacy. In particular, concentrated control over data has enabled dominant firms to capture markets and erect entry barriers, while commercial surveillance has allowed firms to identify and thwart emerging competitive threats”.²³⁷⁸ But there is still an ongoing scientific debate about whether data protection issues should be included in antitrust assessments.²³⁷⁹ Others²³⁸⁰ argued that other authorities besides the lead data protection SA are not competent under the GDPR to sanction data protection breaches. It was also noted that the GDPR has created its own regulatory regime on how breaches of the GDPR should be sanctioned. If national authorities were also able to examine data protection regulations and sanction violations, this regime could be circumvented. On 4 July 2023, the CJEU answered the questions raised by the above-mentioned case of the German Federal Cartel Office (BKartA) and found²³⁸¹ that the authority must examine, based on all circumstances of the individual case, whether the conduct of the dominant company impedes competition by means that deviate from normal product and service competition. For this purpose, the compatibility or incompatibility of such conduct with the GDPR can also be an important indication. If a competition authority takes compatibility and incompatibility with the GDPR into account, this is done exclusively to determine the abuse of a dominant position and to impose competition law measures to remedy the abuse. The competition authority does not thereby take the place of the data protection SA in an impermissible manner and does not make use of powers reserved to the SA under Art. 58 GDPR. The GDPR therefore does not create a blocking effect. However, the CJEU also noted the risk of divergences that may arise when competition authorities and data protection supervisory authorities SAs obliged to coordinate with each other. Specifically, it follows that the competition authority must check whether the conduct at issue has already been the subject of a decision by the data protection SA or the CJEU. If this is the case, it may not deviate from the assessment under data protection law. According to the CJEU, the mere fact that the controller has a dominant

²³⁷⁷ CJEU. (20 September 2022). *Press Release No 158/2*.

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158en.pdf>. P. 1.

²³⁷⁸ USA, FTC. *Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security*, Commission File No. P065401,

https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf, (1 October 2021). P. 2.

²³⁷⁹ Inter alia Buchner, B. [Benedikt]. (2019). *Datenschutz und Kartellrecht. Wettbewerb in Recht und Praxis 2019*, 1243–1248. P. 1244 ff.

²³⁸⁰ Inter alia Piltz, C. [Carlo]. (7 Februar 2019). *Bundeskartellamt erlasst Untersagungsverfügung gegen Facebook – Warum das Vorgehen der Behörde datenschutzrechtlich kritisch betrachtet werden muss*.

<https://www.delegedata.de/2019/02/bundeskartellamt-erlasst-untersagungsverfuegung-gegen-facebook-warum-das-vorgehen-der-behoerde-datenschutzrechtlich-kritisch-betrachtet-werden-muss>.

²³⁸¹ CJEU. Judgment of the Court of 4 July 2023, *Meta Platforms and Others v Bundeskartellamt*, Case C-252/21, ECLI:EU:C:2023:537.

position in the market does not make consent involuntary. On the other hand, there may be a power imbalance vis-à-vis the dominant company as a user, which must be considered when examining consent and, in particular, its voluntariness.

The option through antitrust rules is limited to only a subset of the existing problems, namely that of limiting the market power of different MNEs. Nevertheless, as with the non-legislative approaches, antitrust law elements of national and supranational laws that at least partially fulfill the objectives of an intervention should not be discarded as the “no action” option. Rather, they should still be considered as “best practice” to be included in a possible new regulation.

1.2. International law

However, as examined above, there are good reasons, in particular the need for global harmonization, why a global governance approach might be preferable. Re-considering Rojczak’s approach, this would then be the top-down approach.

The body of rules in the international fundamental rights catalogue with the largest scope of application is the ICCPR. It is an elaboration of the declarations established in the UDHR. Art. 17 ICCPR contains, through interpretations of the UN HRC, the protection of personal data as an element of privacy protection. It thus fulfills the human-centric objective. It also contains legally binding obligations for the Parties to the Covenant. A violation of Art. 17 ICCPR is therefore a violation of the Covenant. However, the ICCPR is insufficient to protect data subject rights in vertical relationships. This is due to the fact that a violation of the Covenant can only be alleged against a State being Party to the Covenant. Data subjects must therefore be able to determine which State is responsible for the violation. This is not reasonably possible in TFPD scenarios. This was apparently recognized by the UN in 2018, when a step in the right direction was taken with the “Working-Draft Legal Instrument on Government-led Surveillance and Privacy”²³⁸² submitted to the UN HRC by the UN Special Rapporteur on the right to privacy. The draft agreement was rejected by the US, China, and by the Member States of the European Union. It could have improved the position of data subjects in vertical relationships. Because of the positions of the US and China, with the former having notified of derogations that deprive it of its actual usefulness at the level of national law and the latter not having ratified the ICCPR at all, is the ICCPR still not a universal treaty and would therefore hinder universality (globality) of a future data protection model as a prerequisite for ensuring its effectiveness. Moreover, due to the generality of the Covenant, a specification of legal safeguards would require a considerable further development of the law and would neglect principles and essential guarantees. It is also difficult for the ICCPR to demonstrate that certain national regulations inadequately protect individual rights. Rojczak had noted that “national law that allows further transfer of data to a third country without due legal safeguards will not infringe Art. 17 because the mere fact of transferring the data does not result in the materialization of the risk of violating privacy”.²³⁸³ Finally, the Covenant “is equipped with a relatively ineffective control mechanism, based on quasi-judicial proceedings conducted by the UN HRC. This procedure is more similar to arbitration, because it requires the consent of the Parties to undergo the procedure, and the resolution of the dispute has no *erga*

²³⁸² UN, Office of the High Commissioner for Human Rights. *Special Rapporteur on the right to privacy presents Draft Legal Instrument on Government-led Surveillance and Privacy*, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf, (28 February 2018).

²³⁸³ Rojczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 28–29.

*omnes*²³⁸⁴ effect in relation to other states' practice."²³⁸⁵ An option via the Covenant alone (without even an additional protocol to the Covenant) would therefore lead to an ineffective control mechanism.

The exercise of national legislative sovereignty could be clarified in another additional protocol to the ICCPR, which was initiated by Brazil and Germany in 2013.²³⁸⁶ It could adapt the scope of data protection to the age of cyberspace and set limitations to State surveillance mechanisms. The content of an additional protocol cannot be laid down by extensive interpretation of Art. 17 ICCPR and needs intergovernmental negotiation. However, this negotiation requires a sufficiently critical mass of the signatory States and therefore usually takes years until consensus can be reached. Moreover, an additional protocol is an instrument that does not bind all signatory States, but only those that are willing to guarantee additional legal safeguards. It would therefore "not solve the problem of the lack of a quick and effective court path in which judgments issued would be effectively *erga omnes* and would contribute to the implementation of uniform standards in all countries with the same data protection regulations"²³⁸⁷. Lastly, it is also questionable whether an additional protocol could lead to harmonization on a scale envisaged by the general objective. The same applies to the use of conflict of laws rules. Although this option would lead to greater legal certainty, it would not solve the problems arising from national substantive law, especially the different levels of data protection.

International conventions open options for influencing the behavior of other States by including data protection matters. If an exchange of personal data is contractually agreed, the obligation to protect personal data is already a *de lege lata* condition for cooperation that an essentially comparable level of data protection must exist in the recipient country;²³⁸⁸ otherwise – as in the relationship between the EU and the US – an adequate level of protection must be ensured through separate agreements. Those can be bilateral or multilateral, whose contents have been described above²³⁸⁹. What needs to be investigated now is whether they could represent viable options.

In the EU-US arena, bilateral agreements include in particular the developments around Privacy Shield 2.0 and the EU-US DPF²³⁹⁰, the EU-US MLAT, the Umbrella Agreement, the EU-US PNR Agreement and the EU-US TFTP Agreement. In the EU arena, these are in particular the specific provisions on data protection in trade agreements with, e.g., Australia, New Zealand, and the UK, as well as the EU-Japan MLAT. However, the improvement of bilateral agreements could not lead to a "substantial part" of the global economy or a "critical mass" of stakeholders being covered. Such an option would also entail the risk that the split between the "groups" a particular state belongs to would become even greater. Such an option would therefore not fulfill the "consensus" and "universality" objectives.

Most multilateral agreements originate from the international trade law domain. These include agreements such as USMCA, CPTPP, RCEP, and NAFTA. However, we agree with UNCTAD, which found that "in view of the different characteristics of data in

²³⁸⁴ Obligations *erga omnes* means that obligations are absolute, for every State, regarding every other State or person.

²³⁸⁵ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 29.

²³⁸⁶ German Federal Foreign Office. (19 December 2013). *German Brazilian resolution on internet privacy adopted*. <https://www.auswaertiges-amt.de/en/aussenpolitik/internationale-organisationen/vereintenationen/131127-resolution-privatsphaere-im-internet/258450>.

²³⁸⁷ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 38.

²³⁸⁸ Art. 44 GDPR, Art. 2(1) Convention 108+, OECD Guidelines 2013 No. 17.

²³⁸⁹ Chapters II-VII

²³⁹⁰ Although Safe Harbor and Privacy Shield were not international agreements in the strict sense of international law, but two unilateral actions.

comparison to goods and services and their multidimensional nature, cross-border data flows require a different treatment from trade in terms of their regulation²³⁹¹. Moreover, such agreements are limited in scope and subject matter and, like bilateral agreements, would not meet the objectives.

The ASEAN and APEC frameworks are also region-based supranational agreements, but their subject-matter focus lies on data protection. There could be an option to more formally integrate and harmonize both frameworks. However, this alone would not be sufficient to achieve the objectives. Rather, multiple integration measures would have to be carried out between existing supranational agreements. This is not the most viable option. Nevertheless, the measures connected to aligning ASEAN and APEC frameworks, including technical, political, and cross-regional adequacy options, may be relevant to the option of enactment of new regulation, and will therefore be discussed in more detail below²³⁹².

The G20 and G7 groups have also recognized the contribution of data protection to trust in the digital economy and data flows, in particular through the concept of DFFT, which has already been described in various places in this thesis. This initiative is also too limited in scope but can play a role in the adoption of new regulations, especially for the “trust” and “cooperation” objectives.

From the WTO domain, GATS only plays a role – albeit an important one – in assessing permitted or non-permitted restrictions on a free flow of data,²³⁹³ so it is not a possible option. The Trade in Services Agreement (TiSA), which includes a commitment to the free flow of data and a ban on data localization, has a potentially wider scope. It draws on the structures of the GATS in its design of the agreement. It was a proposed international trade agreement between 23 Parties, including the EU, the UK and the US. However, it was put on hold in 2016, and a concrete end date for the negotiations is currently not foreseeable. In addition to TiSA, another development from the WTO domain is the “WTO e-commerce talks”²³⁹⁴. These were a promising option. The US Congress had also noted that “Congress also may examine how best to achieve broader consensus on dataflows and privacy at the global level, including through potential common approaches with the EU in ongoing bilateral and multilateral digital trade negotiations [...] including in the OECD and WTO”²³⁹⁵. These talks have not yet been concluded and are therefore not the best option for an intervention. However, UNCTAD noted in this regard that

the outcome of the negotiations can have important implications for the future development of e-commerce and for the evolution of the multilateral trading system. Strong heterogeneity in digital capacities and regulatory preferences among the participating WTO members makes finding common ground on issues such as cross-border data flows a daunting challenge. Non-participation of a significant number of developing countries also raises systemic questions on what kind of format a future agreement could take within the WTO architecture, and what effect it could have on non-participating countries. It is difficult to predict the outcome of these processes at

²³⁹¹ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 75.

²³⁹² Chapter XI, Section III.2.

²³⁹³ See Chapter X, Section II.2.

²³⁹⁴ See Chapter V, Section III.

²³⁹⁵ USA, Congressional Research Service. *U.S.-EU Privacy Shield and Transatlantic Data Flows*, R46917, (22 September 2021). P. 23.

the WTO. An important factor in determining this outcome, however, will be the degree to which similar clauses are inserted in multilateral and bilateral agreements.²³⁹⁶

The OECD Guidelines 2013 have a smaller scope of application than the WTO rules. In the course of the improvements of the 1980 version, the OECD Guidelines 2013 neither included the principles of data minimization nor storage limitation. They also do not regulate two essential guarantees. Finally, the OECD are non-binding.²³⁹⁷ The same applies to the UN Guidelines.²³⁹⁸

There is to date only one instrument that introduced legally binding data protection rules and has an international scope, which is the Convention 108+²³⁹⁹. Another option may therefore be to improve Convention 108+. Bygrave noted in this respect that

yet while there is clearly a need for a global legal approach in the field, there is, realistically, scant chance of, say, a U.N.-sponsored convention being adopted in the short term. The closest to such an instrument at present is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Convention 108+] [...].²⁴⁰⁰

As most of this Convention's Parties are European countries, the fulfillment of the objective of "universal consensus" is doubtful. One option would be to persuade non-Members, especially the US and the EU²⁴⁰¹, to join Convention 108+. Over the last 30 years, however, only a few countries have decided to accede to this Convention. Even if one were to take advantage of the current momentum resulting in particular from the negotiations in the EU-US arena²⁴⁰², and the awareness towards increasing data flow restrictions²⁴⁰³ threatening the global digital economy, an accelerated accession of other countries to Convention 108+ would only make sense if it could fulfill the other objectives in addition to its binding nature. However, the generality of the provisions of the Convention 108 had already led to the fact that the European Community started its own legislative work, resulting in the adoption of Directive 95/46²⁴⁰⁴. Moreover,

the modernized Convention still needs transposition into national law, which means that it is an act addressed to states, not being a source of direct obligations for the entities concerned (e.g., data controllers). An individual cannot, therefore, claim their rights solely²⁴⁰⁵ on the basis of the provisions of Convention 108+. Data controllers are also not obliged to directly apply the above convention's provisions, but to implement the relevant regulations of national law.²⁴⁰⁶

Lastly, although Convention 108+ determines the Parties' SA's as national independent oversight mechanism in Art. 15, it does not provide for the establishment of a dedicated judicial body competent to resolve disputes arising from its application.²⁴⁰⁷ Even if one

²³⁹⁶ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 151.

²³⁹⁷ See Chapter V, Section I.

²³⁹⁸ See Chapter V, Section II.

²³⁹⁹ See Chapter II, Section III.3.

²⁴⁰⁰ Bygrave, L. A. [Lee A.]. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press. P. 181.

²⁴⁰¹ The problem of EU as an "international organization" acceding to Convention 108+ is still pending.

²⁴⁰² See Chapter IX, Section II.1.

²⁴⁰³ See Chapter VIII, Section I.

²⁴⁰⁴ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 29.

²⁴⁰⁵ Such claims are possible in cases of a violation of Art. 8 ECHR according to Art. 34 ECHR.

²⁴⁰⁶ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 30.

²⁴⁰⁷ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 30.

would like to assume that the ECtHR can be considered such a judicial body, because in cases involving an alleged violation of Art. 8 ECHR, the provisions of Convention 108+ are also taken into account, data subjects would still be unable to refer complaints to a supranational controlling body. Data subjects would need to rely on relevant national law or choose a way of claiming their rights in a foreign jurisdiction, which can be a highly obstructive process for those individuals. Therefore, Convention 108+ in its current form is not the most preferable option.

2. Enactment of new regulation

Another option is the unification of substantive law through the enactment of a new regulation within international law. This could take the shape of an agreement that is binding for the Parties (in the Union law, an example would be “Directives”, Art. 288 III TFEU), a binding agreement with direct effect for citizens within the Parties’ territory (in the Union law, an example would be “Regulations”, Art. 288 II TFEU) or a non-binding agreement (an example in the Union law would be “Recommendations and Statements”, Art. 288 V TFEU).

According to the findings in this thesis so far, a non-binding agreement is not an option and must therefore be excluded. A flaw of the ICCPR was noted above that its direct effects only apply to States. To ensure the essential guarantees, which also include the exercise of data subject rights, direct effect for citizens within the Parties’ territory is unavoidable.

The most extreme position would be that an intervention needs the establishment of cyberspace as an autonomous legal space. The Snowden revelations in 2013 led to the discussion if the Internet should be treated as a *res communis omnium*, a common heritage of mankind, and that a possible multilateral regulation of the Internet should be subject to justice to the benefit of all living generations. This parallels, for example, the international law of the sea. If this were followed, then Cyberspace would be exempted from the sovereignty of States and thus from the application of their national laws. In principle, consensus is needed to regulate international domains, based on existing custom. Rojszczak found that “in the case of cyberspace, there is no such custom; nowadays it is difficult to find prohibitions limiting the scope of acceptable use of cyberspace that are actually respected on a global scale.” However, we have shown in the objectives above²⁴⁰⁸ the basis on which consensus might well be possible. However, this alone would not lead to regulatory convergence, but would merely allow for a separate jurisdiction. A solution would thus require an intervention that not only regulates jurisdiction but also harmonizes substantive law.

An international agreement was already called for in 2005. In the Montreux Declaration it was stated that “it is necessary to strengthen the universal character of this right in order to obtain a universal recognition of the principles governing the processing of personal data whilst respecting legal, political, economical and cultural diversities” and appealed to the “United Nations” (UN) “to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human right”.²⁴⁰⁹ This type of agreement was also requested by the former German Chancellor

²⁴⁰⁸ Chapter X

²⁴⁰⁹ ICDPPC. *Montreux Declaration*, https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf, (2005). (“Montreux Declaration”).

Ms. Merkel²⁴¹⁰, and during the 35th ICDPPC.²⁴¹¹ This conference called on governments to create global standards for the protection of personal data through the adoption of an international agreement that could build on the Madrid Resolution from 2009.²⁴¹² Specifically, an additional protocol to Art. 17 of the ICCPR was proposed. Hereby,

interested States would be able to accede to this protocol and, in consequence, jointly create a supra-regional standard for the protection of personal data. Although theoretically possible to implement, this concept has a significant draw-back in the form of a lack of real support from governments [and] even the significant support of data protection ombudsmen to adopt a specific legal international solution does not in any way mean that the proposal will be supported in intergovernmental relations.²⁴¹³

However, a solution via the ICCPR, and even via an additional protocol to the ICCPR, has enforcement flaws, as explained above. Moreover, as Rojszczak also correctly stated,

there would be a real problem with the use of double standards in relation to the provisions of Convention 108+: violations linked to the member states of the Council of Europe would probably be submitted for review to the ECHR, whereas other cases would be handled by the HRC. This, in turn, could lead to a duality of jurisprudence and, in effect, to the application of different data protection standards.²⁴¹⁴

An option aimed at linking the ICCPR to an appropriately adapted Convention 108+ should therefore be rejected.

The question is also which countries should be covered by a new regulation. Atkinson / Cory stated that

ultimately, policymakers need to recognize the critical policy distinction – between policies with global consensus and those without. In many cases, this consensus will (at best) be widespread but not unanimous. Given this reality, it is better that a consensus-based approach be ambitious, but pragmatic, in seeking shared principles and agreements among a like-minded group of countries that represent a substantial part of the global economy and value a mostly open, rules-based global digital economy.²⁴¹⁵

We agree with this only to a limited extent. It is true that consensus²⁴¹⁶ is not equally urgent in every area of regulation. However, as we have seen so far, the field of TFPD requires, e.g., a high degree of legal certainty for actions on the Internet, cooperation between States for law enforcement, and access to information that is not prevented by monopolies or oligopolies. This argues for an equally high degree of harmonized rules. It is therefore not sufficient to agree on a uniform minimum level among such like-minded

²⁴¹⁰ *Frankfurter Allgemeine Zeitung*. (20 July 2013). Merkel regt globales Datenschutz-Abkommen an.

www.faz.net/aktuell/politik/spaehaffaere-merkel-regt-globales-datenschutz-abkommen-an-12288963.html

²⁴¹¹ Hunton & Williams LLP. (2023). *35th International Conference of Data Protection and Privacy Commissioners*.

https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/10/35th_Annual_International_Conference_of_Data_Protection_and_Privacy.pdf

²⁴¹² ICDPPC. *The Madrid Resolution*, [https://edps.europa.eu/sites/edp/files/publication/09-11-](https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf)

[05_madrid_int_standards_en.pdf](https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf), (2009).

²⁴¹³ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 39.

²⁴¹⁴ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 38.

²⁴¹⁵ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer. P. 226.

²⁴¹⁶ See also Chapter X, Section II.1.

group of countries. The objective should be to cover with an intervention all Member States of the UN. Otherwise, the already widening split between the “groups”²⁴¹⁷ a particular State belongs to would become even greater.

We therefore agree with Greenleaf²⁴¹⁸ that the UN should be called upon to create this new regulation. In his opinion, the UN should “accept and advocate that the standards embodied in the Council of Europe data protection Convention 108, including its stronger modernized version, are now international best practice”. Although Convention 108+ contains the same principles and essential guarantees as the rest of the European framework²⁴¹⁹ and would therefore be the most viable starting point as content of an intervention, to achieve the objective of the widest possible coverage of a harmonized level of data protection, more than an extension of the scope and improvement of the rules of Convention 108+ is needed. Convention 108+ would still need transposition into national law, which would run counter to the objectives explained above. However, an intervention should be assigned to an organization that can guarantee this broadest possible scope faster than Convention 108+, which is in our opinion the UN. Although a solution cannot be pursued through the ICCPR alone, as Greenleaf also noted, Art. 17 ICCPR should continue to be aligned with both Convention 108+ and Art. 8 ECHR, and a revision of General Comment 16 would be a simpler and more workable approach than a new General Comment to the ICCPR.

Moreover, if a new regulation also recognizes a certain objective and provides for international cooperation, this can be an indicator when assessing the existence of a “public interest” pursuant to Art. 49(1)(d) GDPR, if the EU or their Member States are a Party to that new regulation. This refers only to public interests that serve an important legal interest. As examples, Recital 112 of the GDPR mentions transfers to international humanitarian organizations for the fulfillment of tasks as defined by the Geneva Conventions or for purposes of international humanitarian law applicable in armed conflicts. For such cases, the exception under Art. 49(1)(f) GDPR may also apply. Also mentioned in Recital 112 are TFPD between competition, tax or customs authorities, between financial SAs or between services responsible for social security matters or public health, for example in the case of combating contagious diseases or doping in sports. We are of the opinion that, since this new regulation would serve the protection of fundamental rights, then, similarly to public health (recognized public interest), data protection as recognized fundamental right in such transfers should also be in the public interest. We also believe that from an EU perspective this transfer is also necessary for the fulfillment of this interest, because the unharmonized global level of data protection which leads to significant problems cannot be remedied in any other way, as mentioned above. This would mean that a TFPD from and to Parties to that new regulation would then also be permitted under the systematics of Chapter V of the GDPR.

IV. Conclusive remarks

What option is supposed to succeed in effectively regulating a global, collaborative medium which is highly flexible because of its fully automated processes, ignores the territorial boundaries, overrides the legal and sociocultural divergences of social orders, and makes the demarcation between State and non-State actors fade? We must think outside the box and avoid regulatory bias, corresponding to the abovementioned specific objective of “innovation”. Although national and supranational law in the aforementioned

²⁴¹⁷ See Chapter IX, Section I.2.1.

²⁴¹⁸ Greenleaf, G. [Graham]. (9 April 2018). The UN Should Adopt Data Protection Convention 108 as a Global Treaty. *UNSW Law Research Paper*, 18(24), <https://ssrn.com/abstract=3159846>.

²⁴¹⁹ See Chapter IX, Section III.2; and Chapter IX, Section III.3.

“leading role” (Rojszczak) are nowadays “the most common ones [and] are based on laws whose scope is only regional, whereas international regulations are applied in a supplementary way”, they would “encounter barriers related to the collision of different legal systems, where it is often impossible to unify substantive regulations because of incompatible political solutions.”²⁴²⁰ These barriers contradict the global, inter-operational nature of information and communication technologies, which transcend borders.

Improving supranational law fails primarily because the ICCPR would have significant enforcement deficits even after an eventual additional protocol. A new regulation in the form of a binding international agreement, based on the content of Convention 108+, adapted to the general objective, the specific objectives and the operational objectives, would therefore bring the biggest improvements and would allow combining the benefits of the various actions discussed in this Chapter XI, as these are complementary. Such new regulation is therefore still the best, albeit the most intrusive, option. To obtain support for such option (objective of consensus), it must nevertheless be made clear to the stakeholders in the global ecosystem of TFPD that their preferred policy option had been considered.²⁴²¹

²⁴²⁰ Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44. P. 37.

²⁴²¹ See also Chapter XII, Section II.

CHAPTER XII: OPERATIONALIZING THE PREFERRED INTERVENTION OPTION

To operationalize the preferred intervention option identified above²⁴²², several steps are necessary. These are determined by the operational objectives, which have been determined above²⁴²³. Operational objectives are to be explained in a different place than the general and specific objectives because the operational objectives are directly linked to the outputs of an intervention and are relevant for a later monitoring and evaluation of the intervention²⁴²⁴. This approach also differs from an intervention that would only define broad policy objectives; the latter would only require general and specific objectives according to the Commission's Better Regulation approach²⁴²⁵.

These steps primarily include the outline²⁴²⁶ of the contents of the intervention in Section III of this Chapter, whereby additional non-legislative actions are also to be included, which were eliminated as a sole option above²⁴²⁷. Furthermore, aspects that were identified above²⁴²⁸ in the context of the objective "maturity" will also be considered. Some aspects of maturity are usually tackled first, while others come later. Setting the rules of the intervention as such should be the first step, because, for example, it would be difficult to set standards for a training program without first enacting the substantive law as such. To enable an advanced and comprehensive framework, planning aspects will also be considered, which could be included in a UN strategy. The intervention could be supported by implementation guidelines, public education measures, and training measures. Moreover, an enforcement authority and coordination mechanisms for government agencies could be defined.

The formation of a uniform law is a challenging solution, which requires the willingness of all aforementioned stakeholders²⁴²⁹ in the different arenas²⁴³⁰ to engage in a discourse. First, the basics of the formation of international uniform law have to be explained.

I. Basics: Building international uniform law

In addition to the supranational level in a region (e.g., EU), there is also uniform law that is globally oriented. Such international uniform law can be intended or unintended, its application can be mandatory or optional. It is clear from the objectives and options

²⁴²² Chapter XI

²⁴²³ Chapter X

²⁴²⁴ Whereas details of monitoring and evaluation (e.g., monitoring indicators, what would be monitored, from when will the monitoring start, by whom and how the results will be used, and when the future evaluation will be undertaken) are not within the scope of this thesis.

²⁴²⁵ See also Chapter I, Section II.4.

²⁴²⁶ An article-by-article proposal of the exact wording of such a new regulation would go beyond the scope of this thesis and has therefore been discarded.

²⁴²⁷ Chapter XI, Section II.

²⁴²⁸ Chapter X, Section II.4.

²⁴²⁹ Chapter IX, Section I.

²⁴³⁰ Chapter IX, Section II.

above that we are aiming at a mandatory, organized, and not only a spontaneous²⁴³¹ or indirect²⁴³² uniform law. International uniform law does not mean that it has come into force in all countries of the world. Even the most successful international conventions have not achieved this goal. Rather, it means that their territorial scope is not limited to States from one region but is in principle accessible to all States of the world. The intervention is intended to unify national laws as much as possible for matters with foreign implications and not for purely domestic matters, because the nature of TFPD is one with foreign implications.²⁴³³

International uniform law is created by international organizations and conferences of States. The form of the intervention could be a multilateral convention, to unify the law of the participating States according to the degree of agreement within the scope of the respective subject matter. A bilateral or plurilateral convention is out of the question because of its limited effect on the unification of law.

Consensus is achieved through concurring declarations of intent by the legal subjects of international law. The latter are, in principle, the Member States of the UN. However, an intervention could also allow region-based organizations such as the EU to sign and ratify. The EU, for example, has such a legal personality and is consequently a subject of international law that can negotiate and conclude international conventions in its own name, i.e., it has competences in this field conferred on it by the EU treaties. Furthermore, unless the subordination of such convention to the law of one of the Parties to that convention is explicit, or clearly follows from the circumstances, it must be assumed that such convention is “determined by international law” between the subjects of international law.

The aim of the intervention is the creation of a legally binding norm and not a mere “gentlemen’s agreement” or “letter of intent”. The UN Charter differentiates between “recommendations” and “decisions”. Resolutions of the UN Security Council, including both Chapter VII resolutions and Chapter VI resolutions (both Chapters of the UN Charter), can theoretically have binding effect. However, whether such resolutions contain a binding decision or only a non-binding recommendation can be difficult to interpret and depends on the individual case. Moreover, it is uncertain whether an intervention would fall within the scope of responsibility of the UN Security Council, which deals with “threats to or breaches of the peace and acts of aggression” on an ad hoc basis. UN Security Council resolutions can therefore also be discarded as an instrument.

Acts of the General Assembly take the form of resolutions, declarations, or decisions. These terms cannot be understood as legal evaluations, not least because their use in the practice of the UN itself is not uniform; “resolution” is often used as a generic term for all three. Resolutions of the General Assembly of the UN are not legally binding as such, they are formally not part of the catalogue of sources of international law in Art. 38 Statute of the ICJ but fall in principle under the concept of soft law.²⁴³⁴ Binding force of the content of a resolution of the General Assembly could nevertheless be caused by the way of a subsequent development of the same legal principle in practice between the States. International custom arises, however, by longer, similar behavior of the involved States (*consuetudo*), connected with the conviction of the States that this

²⁴³¹ Which is not achieved through negotiations and cooperation between several States, but spontaneously through the application of certain standard clauses or standard contracts by many actors.

²⁴³² By using uniform templates in the drafting of new international uniform law or comparative law work in the run-up to the drafting of national laws.

²⁴³³ See Chapter I, Section II.5.6.

²⁴³⁴ Although opinions are increasingly appearing in the literature that the UN General Assembly can establish binding new norms of international law. For example, it is argued that Resolution 2131 established a new rule of international law by way of a binding interpretation of Art. 2(4) of the UN Charter.

behavior is legally required (*opinio iuris*). The time factor with the parallel State practice is thus triggering the binding effect; this contradicts the objectives of the intervention. A new general principle of law can, however, arise directly through the general recognition of the community of States on occasion of the vote in the General Assembly or also outside of it. A resolution of the General Assembly can establish a previously unrecognized general principle of the law in the sense of Art. 38(1)(c) Statute of the ICJ. Some resolutions of the General Assembly – e.g., Resolution 1514 – are sometimes considered to contain a presumption, albeit rebuttable, that the principles incorporated in such a resolution are consistent with universal legal conviction, particularly if the resolution was adopted unanimously in the General Assembly.²⁴³⁵ However, even from this it would not follow that such a resolution by itself establishes law but is merely an important piece of evidence for the existence of a general principle. Those ways of establishing a binding force of the content of a resolution of the General Assembly are not yet conclusively certain enough to base an intervention on this possibility. A Resolution of the General Assembly of the UN should therefore not be used as an instrument for the intervention in question.

Binding force can be established either by the direct effect of the legal act itself or in the form of a national implementing act. Some supra-national organizations (e.g., EU) have the choice between harmonizing acts (e.g., a “Directive” in EU law) and unifying acts (e.g., a “Regulation” in EU law). In the case of a harmonizing legal act, the choice of implementation and the formulation of the national regulations to be observed later by the legal practitioners is left to the Member States. The result is therefore regularly “only” harmonized law. The application and uniform interpretation of this legal act would then be made more difficult by the fact that, within the comparative legal interpretation, the respective national transposition act would have to be found to be able to ascertain the case law and literature of the other contracting States. Furthermore, the respective national transposition act would have to be seen in relation to the underlying text of the legal act to be able to assess whether differences in the respective case law are based on permissible individual deviations of the national legislation from the given supranational norm text or not. In theory, a harmonizing legal act can lead to a high degree of harmonization, but in practice there are major obstacles in its application and interpretation. The goal of the intervention should therefore be a formal unification of law and not merely an approximation of law. “Model laws” are therefore also discarded for an intervention, since such laws are also comparable to Directives in terms of binding effect; here, too, there would be a risk that the individual national laws would deviate considerably from the model law template. The intervention should bind not only States, but also non-State actors. Because “the fulfilment of the vision of the UDHR will remain elusive unless all forms of human rights violations – by States and non-State actors alike – are eliminated and the perpetrators of the violations – whether state or non-state actors – are liable to be held responsible for them”²⁴³⁶. Nothing else may apply to the human-centric intervention in question.

At the global level, international conventions are the most common instruments of unification. From the perspective of international law, they do not require any further implementation measures to establish rights and obligations but are binding immediately upon signature (so-called “self-executing conventions”). Thus, they do not merely contain obligations under international law for the contracting States, but directly applicable rules of substantive law that do not need to be transposed into national law. In this thesis, this type of convention is to be preferred to a “non-self-executing

²⁴³⁵ Heidenstecker, K. [Karin]. (1979). Zur Rechtsverbindlichkeit von Willensakten der Generalversammlung. *Zeitschrift für die Vereinten Nationen und ihre Sonderorganisationen*, 1979(6), 205–210. P. 208.

²⁴³⁶ Chirwa, D. [Danwood]. (2019). State Responsibility for Human Rights. In M. [Manisuli] Ssenyonjo, *International Human Rights Law. Six Decades after the UDHR and Beyond* (pp. 397–410). Routledge. P. 409-410.

convention”, since the latter requires further elaboration by national legislators to establish rights and obligations, and thus would permit only a lower degree of unification. Furthermore, the question arises under which conditions international law has “direct legal effect” for citizens in the form of providing them with legal rights. A prime example of a convention with direct effect is the ECHR.

In legal dogmatics, a distinction is made between a monistic approach and a dualistic approach. In a monistic approach, international law and national law form two parts, with international law taking precedence over national law. An international convention then takes precedence over national law and is binding once ratified, while citizens can directly invoke international law, which national courts are legally bound to apply. Under a dualistic approach, national and international law are not considered part of the same but separate legal orders. Under this approach, international law must first be transposed into national law to become binding in national law. Under this approach, citizens cannot directly invoke international law but must await its implementation, while the same is true for national courts, which are bound only by national law. Above²⁴³⁷, a weakness of Convention 108+ was noted, which is the need to transpose it into national law. The intervention should not replicate this flaw. At this point, the choice between a monistic and a dualistic approach becomes relevant. If an international convention has entered into force but has not been implemented in national law, in a monistic legal system, national courts must still apply the convention, and the State may be held liable to its citizens to the extent that it fails to comply with the international convention. The monistic approach is therefore preferable in this thesis.

Effects of a convention would in principle be *inter omnes*, at least as far as the Member States of the UN are concerned, within the framework of which the treaty text would be adopted. The question remains whether such a convention could give rise to legal obligations not only vis-à-vis States that have signed and ratified the treaty text, but also vis-à-vis other States. States are confronted with a steadily growing number of texts that have been drafted in international organizations and that are qualified in part as binding legal norms with effects *erga omnes*, even if no explicit endorsement by all States of the international community can be demonstrated. An example is the “International Labor Organization” (ILO). The practice of the ILO, based on Art. 19(5) ILO Constitution²⁴³⁸, contains sufficient factors²⁴³⁹ to allow its conventions to be regarded as quasi-legislative acts with effect vis-à-vis all Member States of the organization. Only to the extent that multilateral conventions establish standards that are recognized by international custom they also apply to non-contracting Parties; this is the case for the ILO Constitution. However, this is not the case for any other legal act within the UN. Nor would the intervention be a regulation in the field of *ius cogens*, since not all States have a legal interest in its observance and are therefore entitled to the intervention in the event of violations. This distinguishes the intervention in question from a *ius cogens* minimum standard such as those of genocide, torture, slavery, and systematic racial discrimination.

As a rule, human rights treaties are international conventions between States drawn up in writing, which is why their legal regime is generally governed by the VCLT. VCLT is itself an international convention. The VCLT currently has 116 Parties. In view of this acceptance and the general orientation towards its rules in international legal relations,

²⁴³⁷ Chapter XI, Section III.1.2.; and Chapter XI, Section III.2.

²⁴³⁸ ILO. *ILO Constitution*,

https://www.ilo.org/dyn/normlex/en/f?p=1000:62:0::NO:62:P62_LIST_ENTRIE_ID:2453907:NO, (8 October 2015).

²⁴³⁹ E.g., elaboration of the text in a general conference, adoption with 2/3 majority, involvement not only of State representatives but also of employers' and employees' organizations, delivery of the convention to all Member States with 18-month deadline for ratification.

those of its provisions that were not already international custom are now likely to have become international custom in the majority of cases. In this respect, the rules of the VCLT would also bind non-parties to the VCLT. A prerequisite for this, however, is that a convention is based on a clear intention of the contracting parties to be legally bound. Art. 35 VCLT explicitly requires the consent of a third State when other States provide for a contractual arrangement to the detriment of a third State. An international convention, whatever its content, is therefore without legal effect on States not Party to it.

A legal effect on non-contracting States can thus not follow from the convention itself, but at most by the emergence of a general principle from a convention that was elaborated and adopted in a worldwide framework. In this regard, the ICJ found that “there is no doubt that this process is a perfectly possible one and does from time to time occur; it constitutes indeed one of the recognized methods by which new rules of customary international law may be formed”²⁴⁴⁰. However, the mere vote in an international body with worldwide composition cannot be sufficient for this, because then ratification would be unacceptably redundant.

In international law practice, two treaty conclusion procedures have emerged for negotiating a treaty text causing binding effect: the “composite (multi-phase)” and the “simple” procedure. The simple procedure is used for administrative and less important treaties, which become binding as soon as they are signed by the executive body authorized to conclude them, Art. 12 VCLT. The composite procedure, which takes its name from the various procedural stages under Arts. 9ff. VCLT, is applied to treaties of particular political importance. Human rights treaties are instruments of international law-making in the general interest (so-called “law-making treaties”) and are concluded in the composite procedure. Because of the human centric orientation, we see the intervention as an international convention of more than minor importance and therefore expect a composite procedure. Inserted in this procedure would then be domestic consent and ratification procedures of the Parties.

However, ratification of a human rights treaty does not necessarily mean that it will enter into force. According to Art. 24(1) VCLT, a treaty only enters into force in accordance with the agreement reached. Since we are striving for a convention under the UN, this is dependent on UN law-making procedures. For the ICCPR elaborated in 1966, it was determined that this Covenant requires a number of 35 ratification instruments. Similar could apply to the intervention in question in this thesis. To mitigate a “limbo” between the ratification phase and the entry into force, which is characterized by legal uncertainty, three principles of the VCLT could be included in the intervention: Art. 18(b) VCLT provides for an “interim obligation” for States to refrain from acts which would defeat the object and purpose of a treaty between its signature and ratification; in addition, Art. 25 VCLT provides for the possibility of provisional application of a treaty; lastly, once a human rights treaty has entered into force, its norms must be observed, this principle *pacta sunt servanda* (Art. 26 VCLT) is the authoritative pillar of international treaty law.

II. Process: UN law-making

According to Art. 7(1) UN Charter, the UN has six principal organs: a General Assembly, a Security Council, an Economic and Social Council, a Trusteeship Council, an International Court of Justice, and a Secretariat. The promotion of the progressive development and codification of international law is largely entrusted to the ILC, Art. 13

²⁴⁴⁰ ICJ. *North Sea Continental Shelf Cases*, Judgment of 20 February 1969, Reports of judgments, advisory opinions and orders. P. 41

(1)(a) UN Charter. The ILC is a subsidiary body of the General Assembly, composed of independent “special rapporteurs”. The drafts of the ILC are then submitted to the General Assembly in the form of a final draft. The General Assembly then recommends to the Member States of the UN to sign and ratify.

According to the specific objective “trust”²⁴⁴¹, the intervention also needs an innovative standard-setting process. The intervention should therefore be “enacted in a transparent manner that allows opportunities for broad stakeholder input; [be] evidence-based and consider the technical and economic feasibility of requirements; require the publication of impact assessments to ensure the appropriateness and effectiveness of regulatory approaches; and [be] targeted and proportionate”²⁴⁴². This is also consistent with the Commission’s Better Regulation approach, which provides that “being clearly visible to the outside world is important if initiatives are to be understood and credible. Results of evaluations, impact assessments and consultations could be widely disseminated. Stakeholder responses should be acknowledged, and consultation results widely disseminated through a single access point. The reasons for disagreeing with dissenting views should be explained.”²⁴⁴³ In particular, stakeholders could be invited to actively participate in those areas in the intervention where there is a higher risk of no consensus being reached, or they could even be given priority in the regulatory process. In this way, blockade attitudes from relevant stakeholders could be prevented.

In this process, the UN could integrate consultation with public and private sectors, as well as civil society. Engaging with these is important to understand what is practical and what can be executed, as well as to learn about the stakeholder interests involved. Moreover, when stakeholders are aware of the rules of the intervention and their rights deriving from it, this could create a collaborative enforcement mechanism and ultimately improve the effectiveness of the intervention. Raising awareness for the purposes of the intervention could be done through a public education and awareness campaign. It should be avoided that, despite promising rules as such, the intervention fails due to an insufficiently predefined implementation process and a lack of administrative capacity. UNCTAD also noted the danger that experts in this field rarely devote themselves to the process of a previously identified policy solution.²⁴⁴⁴

A UN strategy could include guidance regarding timeframes for particular provisions to take effect, clarifications on definitions, and published case studies to highlight regulatory interpretations of the law. These can be helpful in providing further context and clarifications of the intervention and reduce uncertainty for legal entities that will be subject to the same. For both in-scope scenarios and scenarios with external relationship, guidance could include on how different government agencies of the Parties to the intervention coordinate for effective implementation of the intervention. Given the complexity of the matter to even reach a consensus for the ruleset, governments of the Parties to the intervention will possibly require certain mechanisms that designate and assign responsibilities among bodies for aspects of, e.g., monitoring and enforcement of the intervention, because these mechanisms will probably have effects on a Parties’ national strategy, and usually require changes in domestic government processes or the establishment of new lines of communication.

²⁴⁴¹ Chapter X, Section II.5.

²⁴⁴² WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 18.

²⁴⁴³ European Commission. *Better regulation toolbox - November 2021 edition*. https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021). P. 7.

²⁴⁴⁴ UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 61.

The strategy could include measures to build resources, knowledge related to data protection, and coordination among UN bodies involved in the intervention. There could also be clear definitions of the roles of these bodies and these bodies could be given appropriate authority to enforce these roles. Staff of these bodies could receive ongoing training on data protection principles together with appropriate manuals.

In order not to jeopardize innovation²⁴⁴⁵ in using personal data, it is to be considered to allow in the intervention a controlled environment. This environment could deviate from certain obligations or sanctions, determine a time of partial or full effect of the intervention, or be used first between a “critical mass” of States for experimenting with the regulatory concept, at least as a steppingstone towards a formal mechanism in the introduction phase of the intervention.

In principle, the intervention would remain in force until amended, revised, reformed, or repealed. Through the inclusion of a sunset clause, the duration of the intervention could be defined and thus the intervention be of temporary nature with a limited lifespan, opposed to permanent treaties, which aim to stay in force perpetually.²⁴⁴⁶ This temporary period could be combined with an evaluation before the deadline expires. In international law,

the use and utility of sunset clauses have remained largely unnoticed despite the fact that they have frequently been employed in major international treaties and agreements. [...] Recently, sunset clauses were also included in major multilateral trade agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) [...] and the Canada – EU Comprehensive Economic and Trade Agreement (CETA).²⁴⁴⁷

Other approaches are so-called “opting-in and opting-out rules”, through which companies have the choice of subjecting themselves to regulation or not; however, those are not further considered in this thesis, as they would contradict the desired self-executing binding effect of the intervention. After the UK Brexit, a so-called “adequacy light” concept has been used. The UK-EU trade agreement stated that transfers of personal data from the EU (and other EEA states) to the UK will not be treated as a transfer to a third country for an initial period of four months, extendable by a further two months unless either party objects. Under this interim adequacy “bridge” the EU was able to continue to treat the UK as an adequate jurisdiction. Some countries such as France and Singapore, but also the EU within its “Data Strategy”²⁴⁴⁸, are familiar with the instrument of a so-called “regulatory sandbox”. Since it is difficult, according to the Commission, to fully grasp all elements of a transformation to a data-agile economy, the Commission wanted to “deliberately abstain from overly detailed, heavy-handed ex ante regulation, and will prefer an agile approach to governance that favors experimentation (such as regulatory sandboxes), iteration, and differentiation”²⁴⁴⁹. Such regulatory sandbox refers to “experimental articles” that enable regulators in cooperation with the businesses and the citizens to test innovative business models. One recent use of a

²⁴⁴⁵ The specific objective “innovation” has been addressed in Chapter X, Section II.7.

²⁴⁴⁶ European Parliament. *Sunset Clauses in International Law and their Consequences for EU Law*, PE 703.592, [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703592/IPOL_STU\(2022\)703592_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703592/IPOL_STU(2022)703592_EN.pdf), (4 January 2022). P 10–11.

²⁴⁴⁷ European Parliament. *Sunset Clauses in International Law and their Consequences for EU Law*, PE 703.592, [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703592/IPOL_STU\(2022\)703592_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703592/IPOL_STU(2022)703592_EN.pdf), (4 January 2022). P 20–21.

²⁴⁴⁸ See above Chapter II, Section II.3.8.2.

²⁴⁴⁹ European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data*, COM(2020) 66 final, (19 February 2020). P. 12.

regulatory sandbox in the European framework was made for the proposed Artificial Intelligence Act.²⁴⁵⁰ In it, the Commission described its concept as contributing

to the objective to create a legal framework that is innovation-friendly, future-proof and resilient to disruption. To that end, it encourages national competent authorities to set up regulatory sandboxes and sets a basic framework in terms of governance, supervision and liability. AI regulatory sandboxes establish a controlled environment to test innovative technologies for a limited time on the basis of a testing plan agreed with the competent authorities.²⁴⁵¹

Within the APAC framework, a similar construct was called for under the name “Regulatory Pilot Space” (RPS).²⁴⁵²

Above²⁴⁵³, strategic policies on data governance for important areas of economic development based on the use of personal data were examined. It was recognized that the three most important frameworks cover with their strategic policies almost all data-driven areas.²⁴⁵⁴ These areas are predestined to be subjected to a regulatory sandbox in the event of a difficult consensus on the rules in an intervention related to such areas. This could allow personal data of these areas to flow freely between countries participating in this controlled environment and give national regulators a more significant role, as Art. 53 of the Commission’s Artificial Intelligence Act does for AI research. In this way, the policy solution in these areas could be tested “to facilitate cross-border data flows and drive digital innovation while protecting consumers”, industry could be given “the option to modify their solutions before bringing them to market if they are deemed unacceptable by the regulator”, and States and the private sector could be enabled to “improve their digital competitiveness”.²⁴⁵⁵ Ultimately, a regulatory sandbox would also be in line with the specific objective of “cooperation”²⁴⁵⁶, as it would diminish a top-down approach – which the GDPR in particular has been accused of.

Providing the intervention with a sunset clause would have the disadvantage that a convention drafted with considerable effort would be threatened by the fact that such clause would provide for an automatic repeal of the entire intervention or sections of the intervention once a specific date is reached. In our view, however, this is outweighed by the fact that, especially in a dynamic regulatory topic such as the TFPD, an international convention would in turn have to be reviewed in a transparent multi-stakeholder process in line with the “multi-stakeholder approach”²⁴⁵⁷. This would make the intervention more responsive to the latest developments in all four dimensions mentioned above²⁴⁵⁸, thus satisfying more stakeholders and increasing the likelihood of an ongoing stable consensus.

²⁴⁵⁰ Bertuzzi, L. [Luca]. (19 October 2022). *EU Council nears common position on AI Act in semi-final text*.

<https://www.euractiv.com/section/digital/news/eu-council-nears-common-position-on-ai-act-in-semi-final-text>.

²⁴⁵¹ EU. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM(2021) 206 final (21 April 2021). P. 15

²⁴⁵² GSMA. (July 2019). *Operationalizing the ASEAN Framework on Digital Data Governance. A Regulatory Pilot Space for Cross-Border Data Flows*. https://www.gsma.com/asia-pacific/wp-content/uploads/2019/11/Operationalising-the-ASEAN-Framework-on-Digital-Data-Governance_WEB.pdf.

²⁴⁵³ Chapter IX, Section III.1.5.

²⁴⁵⁴ China: No Open Data Strategy. US: No comprehensive and consistent strategy on Industry 4.0 / Manufacturing 4.0 / IoT.

²⁴⁵⁵ GSMA. (July 2019). *Operationalizing the ASEAN Framework on Digital Data Governance. A Regulatory Pilot Space for Cross-Border Data Flows*. https://www.gsma.com/asia-pacific/wp-content/uploads/2019/11/Operationalising-the-ASEAN-Framework-on-Digital-Data-Governance_WEB.pdf.

²⁴⁵⁶ Chapter X, Section II.6.

²⁴⁵⁷ See Chapter I, Section II.4.

²⁴⁵⁸ Chapter I, Section I.

An “adequacy light” approach could also be considered, at least for a transitional period and for certain countries. TFPD scenarios between countries in-scope that have already reached an advanced level (GSMA classification), including the EU Member States, the US, and China,²⁴⁵⁹ and all other countries in-scope would be predestined for this. It is also conceivable to pursue this approach for scenarios with external relationship, i.e., for onward transfers of personal data.

III. Instrument: Improved Convention 108+ ruleset

The substantive rules of the most preferable option²⁴⁶⁰ for an intervention strive that the Parties to the intervention not only agree on common rules regarding some matters, but that the solution presupposes a compromise on all issues to become workable. Our claim is ultimately a “full consensus”. In our opinion, this can only be achieved by a mixture of legislative and non-legislative elements. Our solution is also based on the assumption that such consensus can only be reached on the aforementioned objectives²⁴⁶¹, based on the aforementioned interests²⁴⁶². It could then be possible that every dispute within the subject matter of this thesis can be settled by one element within the catalogue of international law sources.

We believe that there is then no need to leave certain sectors open for future negotiations; and that there are also no remaining issues on which the Parties to the intervention would have to agree on in their exercise of jurisdiction and if they deem their national law applicable. Thus, with the chosen option of intervention, it does not have to be decided which States can agree upon rules that reflect their preferences, which State has a stronger interest, respectively closer connection to a specific dispute, and, ultimately, “links” to their national law therefore do not need to be examined. Our solution therefore does not fall under the group of proposals requiring mutually exclusive jurisdictional rules, because there would be no room for conflict of substantial rules, as each issue would be governed by the same uniform rules.

As stated above²⁴⁶³, Convention 108+ can cover positive elements that might be used for an intervention. These are to be described as well as those negative elements²⁴⁶⁴ which might need to be improved. Furthermore, this Section III will analyze elements that may not yet be regulated by Convention 108+ and thus would need to be created in an intervention.

1. Legislative elements

On the positive side, Convention 108+ is intended to facilitate a free flow of personal data while guaranteeing effective protection mechanisms for the use of personal data; this corresponds with the general objective²⁴⁶⁵. Convention 108+ forms a bridge between different regions of the world and, respectively, different normative frameworks. It is applicable to data processing activities carried out in both the public and private sectors. It therefore has the potential of a universal²⁴⁶⁶ approach. Convention 108+ has not only been ratified by all CoE Member States but is also not limited to those. It is open to

²⁴⁵⁹ See Chapter IX, Section III.1.5.

²⁴⁶⁰ See Chapter XI

²⁴⁶¹ See Chapter X

²⁴⁶² See Chapter IX

²⁴⁶³ Chapter II, Section III.3.

²⁴⁶⁴ See Chapter II, Section III.3.

²⁴⁶⁵ See Chapter X, Section I.

²⁴⁶⁶ See Chapter X, Section II.2.

accession by non-member States, even non-European States, if they have been formally invited to accede by the Committee of Ministers of the CoE, Art. 23 Convention 108+.

Even if ratification by more Parties to Convention 108+ would take some time, with currently 44 accessions to this convention, although 7 signatures not followed by ratifications,²⁴⁶⁷ Convention 108+ has – from this aspect – the potential to form the instrument of the preferred intervention option. Convention 108+ is the first international convention in the field of data protection that has a binding effect on the Parties. The preamble of Convention 108+ affirms “that it is necessary to secure the human dignity and protection of human rights and fundamental freedoms of every individual [...]”. It thus has, besides its binding nature, a human centric approach. Convention 108+ contains the same data protection principles²⁴⁶⁸ and essential guarantees²⁴⁶⁹ as the GDPR. There would also be no need to change the legal definitions of Convention 108+, as they are largely consistent with the GDPR, the Charter and the OECD Guidelines 1980.

On the negative side, among the Parties to Convention 108+ are only five non-European States (Cape Verde, Mauritius, Mexico, Senegal and Tunisia), which illustrates that it is still a long run until Convention 108+ could reach importance to such extent that it encompasses all States which have a greater impact on global data protection practice, such as the US and China. Exemplarily, China has been the second largest economy in the world after the US since 2010, and the largest since 2014 in purchasing power²⁴⁷⁰, but both the US and China are not yet Parties to Convention 108+.

In addition, if Convention 108+ were adopted unchanged as an instrument for intervention, a recourse would only be available based on an alleged violation of the ECHR. A consensus on such intervention based on Convention 108+ would then be jeopardized, as non-EU States, which are to be invited to accede to Convention 108+, would then need to accept a possible influence of the CJEU due to ongoing discussions of the relationship between the CJEU and the ECtHR. The ECtHR is linked to the CoE through several provisions in the ECHR, but Arts. 22, 23, 46 and 50 ECHR contain only organizational matters, in particular expenditures of the ECtHR. The question as to whether the ECtHR is an organ of the CoE is still unclear. Equally difficult is the relationship on the legal subject-matter side. T-PD argued that the ECtHR may decide to sanction a Party to the ECHR for reasons connected with its regulation of data protection.²⁴⁷¹ We don't follow this opinion, a direct recourse to the ECtHR based on an alleged violation of Convention 108+ is therefore not possible. There is therefore a “lack of mechanisms for citizens of countries outside Europe to enforce the Convention, including their inability to take cases to the European Court of Human Rights because the European Convention on Human Rights is a closed convention to which non-European states cannot accede”²⁴⁷². To approach this problem by combining Convention 108+ with the ICCPR and an additional protocol was rejected above²⁴⁷³. In the intervention, a similar problem of a judicial redress should be avoided. Art. 12 Convention 108+ stipulates that sanctions and remedies shall be both judicial and non-judicial. However, it does not require that data subjects have a direct right to sue in a civil action in court. The goal for judicial redress should be to find a way comparable with the appeal to the ECtHR also for individuals outside Europe seeking genuine means of redress.

²⁴⁶⁷ CoE. (28 July 2023). *Chart of signatures and ratifications of Treaty 181*. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=181>.

²⁴⁶⁸ See Chapter IX, Section III.2.

²⁴⁶⁹ See Chapter IX, Section III.3.

²⁴⁷⁰ See Chapter I, Section I.2.

²⁴⁷¹ ECtHR. Judgment of 4 May 2000, *Rotaru v. Romania*, Application 28341/95. Para. 43.

²⁴⁷² Greenleaf, G. [Graham]. The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, 2(2), 68–92. P. 88.

²⁴⁷³ Chapter XI, Section III.2.

For the fulfillment of these duties, we believe it is not sufficient to empower a UN committee or the Council of Ministers to receive communications from individuals, civil society organizations, or corporations who wish to complain that a Party to the intervention is not complying with its terms, because all such a body could do “is resort to persuasion or public criticism of recalcitrant countries”²⁴⁷⁴. The Explanatory Report to Convention 108+ also focuses in Recitals 12, 125, 127 and 128 on the cooperation between SAs and the principle of transparency. This could lead to national SAs being overwhelmed by these duties and would need to be resolved through the intervention.

Convention 108+ mentions the criterion “in a democratic society” in several places. It was found above²⁴⁷⁵ that this criterion is not tenable for an intervention, but could rather be replaced by morality, public order, and the common good, as the UDHR does.

The most difficult hurdle that improved rules based on Convention 108+ would have to overcome is the transfer mechanism. It was found above²⁴⁷⁶ that the prohibition principle of the GDPR should only be adopted in an intervention for certain types of data, if at all. The question is for which types of data it could be deviated from the principle of a free TFPD. A distinction could be made between transfers to in-scope countries²⁴⁷⁷, transfers with external relationship²⁴⁷⁸, and all other TFPD scenarios. It should be noted that we are herewith referring to the “second stage” of the test of the lawfulness of a TFPD, not to the “first stage test”²⁴⁷⁹.

From the viewpoint of the geographic scope of the intervention, a transfer to in-scope countries would encompass all Parties to the intervention. A prohibition principle would not be tenable here since the substantive law of these Parties would be harmonized by the intervention. Art. 14(1) Convention 108+ standardizes the fundamental prohibition of data transfers to countries that are party to the Convention. A mechanism including a general free flow of personal data between these Parties and a principle of prohibition on data localization is preferable. However, this free flow would not correspond to a “unilateral openness”, but to an ex-post accountability (also called “light touch” or “organizationally based”) mechanism²⁴⁸⁰. Since the unification of substantive rules would reduce the exposure to legal certainty for all stakeholders, such a mechanism would, in our opinion, be sufficient for transfers between in-scope countries and would not burden these transfers too much due to its low level of restrictiveness. Hereby, an intervention would also be risk oriented. Another advantage would be that “a country’s data-protection rules would travel with the data.”²⁴⁸¹

However, even in the case of transfers to in-scope countries, deviations from this mechanism could be standardized in an intervention; these would then apply all the more to transfers with external relationship.²⁴⁸² China defined various data flow restrictions for specific data types and sectors.²⁴⁸³ The categorization of these types could be based on the most recent regulatory instruments from the Chinese legal sphere.²⁴⁸⁴ “Important

²⁴⁷⁴ Greenleaf, G. [Graham]. The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, 2(2), 68–92. P. 88.

²⁴⁷⁵ Chapter X, Section II.3.

²⁴⁷⁶ Chapter X, Section II.3.

²⁴⁷⁷ See Chapter X, Section II.6.

²⁴⁷⁸ See Chapter X, Section II.6.

²⁴⁷⁹ See Chapter II, Section II.3.1.; and Chapter II, Section II.3.4.4.a.

²⁴⁸⁰ See Chapter IX, Section III.1.4.1.

²⁴⁸¹ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²⁴⁸² See further below in this Section.

²⁴⁸³ See Chapter IX, Section III.1.2.

²⁴⁸⁴ See Chapter IV, Section IV.5.

data” still does not have a precise definition, so this category cannot be adopted for the intervention. “Core data” as a subset of important data, however, could be determined in an intervention as “data related to national security, lifeline of national economy, people’s livelihood and vital public interests” that, if misused, could pose a “serious threat to national interests” by, for example, leading to major damage, leading to large-scale shutdowns, or large-scale network and service paralysis. Convention 108+ lists national security, defense, investigation and prosecution of criminal offences as being excluded. Similarly does the GDPR. If one were to adopt this category in an intervention as a permitted exception to a free flow and ex-post accountability approach, one would cover the rationale “national security / public order / sovereignty”²⁴⁸⁵ (however, this does not apply to the rationales “national digital economy / economic development” and “adequacy and gaps in coverage / citizens’ protection” for reasons mentioned above²⁴⁸⁶) in the sense of the specific objective “universality”²⁴⁸⁷. This could bring us closer to a consensus for a deviation from a free flow principle.

Above²⁴⁸⁸ it was stated that law enforcement purposes fall under the rationale of “public order”. Rules in an intervention regarding law enforcement purposes should lead to mutual benefits for enforcing States in implementing a common mechanism. The existing mechanism for international law enforcement is too slow and dependent on the existence of corresponding MLATs and the will as well as the possibilities of local law enforcement authorities.²⁴⁸⁹ This endangers the interests of enforcement authorities in establishing closer cooperation among SAs to provide both more effective protection of individual rights and greater legal certainty for businesses; as well as the interests of businesses in more legal certainty in cross-border jurisdictional disputes. The fact that possible instruments for this have not been used sufficiently to date has led to new initiatives such as the E-Evidence Regulation. In the intervention, questions of jurisdiction, cooperation of international law enforcement requests, and limits for unnecessary government access to personal data of citizens of other countries should be solved.²⁴⁹⁰ Therefore, intervention rules could be included to

make sure Parties to those agreements do not have it both ways – in terms of having an executive agreement with the United States and other countries to facilitate more efficient access to data in their jurisdictions, while also forcing firms to store data locally to facilitate government access. Including this explicit provision would create a situation whereby there would be no benefit to data localization when it comes to law enforcement access to data.²⁴⁹¹

Aforementioned data type classification could be used to allow certain data flow restrictions in a law enforcement scenario. This rule-exception-model between a general prohibition of data flow restrictions and allowed exceptions could ensure that none of those responsible for the data processing can escape an obligation of a nations’ law enforcement laws by transferring data transborder. In law enforcement scenarios, it is likely that several legal systems have to be considered, because MNEs offering services over the Internet leads to more countries having interests in the same data.

This can place a burden on MNEs and endanger the consensus of these stakeholders. If the regulatory model of obliging ISPs to provide foreign data would be retained, a

²⁴⁸⁵ See Chapter VIII, Section I.2.

²⁴⁸⁶ See Chapter VIII, Section I.

²⁴⁸⁷ See Chapter X, Section II.2.

²⁴⁸⁸ Chapter X, Section II.2.

²⁴⁸⁹ See Chapter II, Section II.3.7.; and Chapter IX, Section I.1.1.

²⁴⁹⁰ See Chapter X, Section II.6.

²⁴⁹¹ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

protective mechanism for transborder data access could be added in an intervention in connection with law enforcement scenarios. Such a mechanism could consist of a “comity analysis”, the criteria for which could be taken from the US Cloud Act;²⁴⁹² but it could also consist of notice requirements. Provided that the data subjects are sufficiently informed and a corresponding practice under international law is in place, in the case of access to personal data whose localization takes place quasi arbitrarily with the knowledge and intention of the data subjects, notification of the State in which the data are actually located could be dispensed. If, however, sufficient clarification has not been provided and if foreign data subjects are affected, notification of the home State of the data subjects could be included as an obligation. If data are stored in a specific location with the knowledge and intention of the data subjects, the obligatory notification of the country in which personal data are located could also be included in the intervention. The requirements and consequences of this notification should anyhow be determined in detail. It should be possible for the notified State to prevent personal data already transferred by an ISP from being used and exploited despite an objection by the notified State. It could also be specified that authorities must comply with their counterparts’ lawful requests for personal data in a timely fashion, unless those requests would violate mutually agreed provisions, such as for national security rationales. Finally, for reasons of transparency, countries could be obliged to report the number of requests they receive, the number of requests they fulfill, response times, and progress in their modernization efforts. If this protective mechanism were not respected, such access would then be an excessive exercise of sovereignty, a jurisdictional overreach.²⁴⁹³

The principle should be, despite the disadvantages of EIOs and MLATs,²⁴⁹⁴ that the acquisition of personal data should be done through the channels of EIOs and MLATs. By addressing both in an intervention, these mechanisms could not be excluded entirely but improved. Not only future, but also existing agreements on law enforcement could be included; the latter include in particular the US MLAT and the EU-Japan MLAT,²⁴⁹⁵ as well as the “executive agreements” under the US Cloud Act.²⁴⁹⁶ The intervention could also include an obligation for Parties to the intervention to strengthen domestic law enforcement processes by ensuring that “domestic institutions that manage foreign governments” requests for data are efficient and well-funded²⁴⁹⁷. The intervention could also provide a model language for new MLATs so that “countries can put in place the individual building blocks that support the longer-term goal of a new multilateral agreement”²⁴⁹⁸. Companies in countries being Parties to the intervention could then generally be obliged to refuse direct requests and refer the requesting third country authority to an existing MLAT.²⁴⁹⁹ A direct transfer by a company to authorities of a third country could only be permitted in particularly urgent cases, e.g., questions of life and death. In this way, the intervention could ensure uniform international regulation of access to personal data in law enforcement scenarios, improve international mutual legal assistance and correspond to the specific objective of “cooperation”²⁵⁰⁰.

²⁴⁹² See Chapter III, Section II.1.2.7.

²⁴⁹³ See Chapter VIII, Section III.

²⁴⁹⁴ See Chapter II, Section II.3.7.; and Chapter IX, Section I.1.1.

²⁴⁹⁵ See Chapter II, Section II.3.7.

²⁴⁹⁶ See Chapter III, Section II.1.2.7.

²⁴⁹⁷ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²⁴⁹⁸ Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.

²⁴⁹⁹ Kuner, C. [Christopher]. (2020). Art. 48. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 825–840). Oxford University Press. P. 833.

²⁵⁰⁰ See Chapter X, Section II.6.

In addition to the rationale “national security / public order / sovereignty”, which focuses on the interests of the stakeholder “State”, there are, however, two other categories for possible deviations from a general prohibition of data flow restriction. First, the category of “universal bads” we had talked about above²⁵⁰¹. Child pornography, for example, is a generally recognized “universal bad” and could therefore justify data flow restrictions in an intervention. Policies on core Internet architecture and protocols is an example of a universal good and should not limit a free flow.

On the other hand, there is the category “sensitive personal data”, which focuses on the interests of the stakeholder “citizen”. The intervention should be based on the list in Art. 9 GDPR, which establishes special categories that require extra attention. However, this last possibility of deviation from the principle of a free flow of personal data should not be designed in such a way that a data flow restriction is permitted, but rather that such TFPD must be specially protected. The European framework lately pushed for data flow restrictions according to data type, and this not only *de facto* (as in the GDPR), but explicitly regulated. Although the GDPR is, at least in theory, the opposite of a data flow restriction regime, since it was designed to allow for TFPD while ensuring that personal data are protected essentially equivalent as if it were in the EU, the Commission recently proposed data storage requirements. Art. 17(1)(c) of the Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union²⁵⁰² provides that “sensitive non-classified information should be stored and processed in the EU”. In the EDPS and EDPB joint opinion on the EU Health Data Space legislative proposal²⁵⁰³ “the authorities urge the legislator to introduce localization requirements for health data. [...] European DPAs [SAs] seem increasingly in favor of data localization requirements that go hand-in-hand with the current political agenda in Brussels, even for countries with an adequate data protection level”²⁵⁰⁴. We do not think that “sensitive personal data” in the sense of Art. 9 GDPR (e.g., health data) is sufficient to justify data flow restrictions for in-scope transfers. A similar view was taken in the conclusions of a G7 meeting, in which the EDPS Mr. Wiewiórowski commented that “even with data-transfer agreements that smooth international business for many companies, some sensitive data such as national security information might need to remain in one jurisdiction”²⁵⁰⁵. This is the crux of the matter at this point. “Sensitive” meant in the sense of “national security / public order / sovereignty” rationale, but not in the sense of the Art. 9 GDPR classification.

However, this rule-exception-model should look different for transfer scenarios with external relationship. Here, there is an increased risk for all stakeholders due to non-unification of substantive law. In our view, this might even justify data flow restrictions for “sensitive personal data” within the meaning of Art. 9 GDPR.

Furthermore, for transfers with external relationship even another default position comes into play. We are of the opinion that for all three data types mentioned above (“national security / public order / sovereignty”, “universal bads”, “sensitive personal data”) a prohibition principle could be the default position in an intervention.

²⁵⁰¹ Chapter X, Section II.1.

²⁵⁰² European Commission. *Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union*, COM/2022/119 final, Procedure 2022/0084/COD, (22 March 2022).

²⁵⁰³ EDPB. *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, (12 July 2022).

²⁵⁰⁴ Bertuzzi, L. [Luca]. (23 August 2022). *Is data localization coming to Europe?*. <https://iapp.org/news/a/is-data-localization-coming-to-europe>.

²⁵⁰⁵ Stupp, C. [Catherine]. (9 September 2022). *G-7 Privacy Regulators Aim To Ease Turbulent International Data Flows*. *The Wall Street Journal*. <https://www.wsj.com/articles/g-7-privacy-regulators-aim-to-ease-turbulent-international-data-flows-11662730512>.

This prohibition principle could only be diminished by a “flow conditional on safeguards mechanism” (also called “based on legitimate grounds”, “prescriptive regulatory approach” or “geographically based mechanism”), which represents the middle of the spectrum of restrictiveness.²⁵⁰⁶ Moreover, this is the most frequently used in practice.²⁵⁰⁷ The requirements of this mechanism should then apply to both the recipient country and the data exporter.

A transfer to out-of-scope countries could then be allowed as soon as importing country has an “essentially equivalent / adequate level of protection”. In this context, it is important to distinguish between “adequacy” and “equivalence”.

Today, only a few countries outline the substantive criteria used to determine adequacy in their data protection regulations. [...] Adequacy and equivalence do not necessarily mean the same thing. Equivalence implies the assessment of a level of objective similarity between two regulations, both in terms of the tools used and the objectives or outcomes of the regulation. Adequacy, in turn, can be more flexible as it implies agreeing on a common outcome but allowing for different tools to be used to meet this outcome.²⁵⁰⁸

We agree with the use of the term “adequacy” for an intervention; also to give room for non-legislative elements²⁵⁰⁹. When determining adequacy, both subcategories²⁵¹⁰ of determining adequacy could be integrated in the intervention. This means that on the one hand the data exporter could determine adequacy through a TIA. On the other hand, an adequacy decision could be made by a body of the UN; considering the proposed separation between consultative body and enforcing body, this could be the UN HRC. This decision could either be established by unilateral recognition of the exporting country for the outbound data flow or it could take the form of a mutual recognition of data protection measures for a TFPD in both directions. This mechanism is being recognized more and more around the world and increases the chance for *consensus* on this. 74 jurisdictions now delegate to either the domestic SA or a governmental authority the power to designate other jurisdictions as having “adequate” data protection standards:

²⁵⁰⁶ See Chapter IX, Section III.1.4.1.

²⁵⁰⁷ According to UNCTAD, these countries have adopted some form of prescriptive regulatory frameworks on transborder data flows: Algeria, Argentina, Armenia, Brazil, Colombia, Côte d'Ivoire, Egypt, EU, Georgia, Israel, Kenya, Malaysia, Morocco, Peru, South Africa, Switzerland, Thailand, Tunisia, Ukraine, United Kingdom, Azerbaijan, Bahrain, Ghana, Japan, Kyrgyzstan, New Zealand, Republic of Korea, United Arab Emirates. See UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>. P. 136.

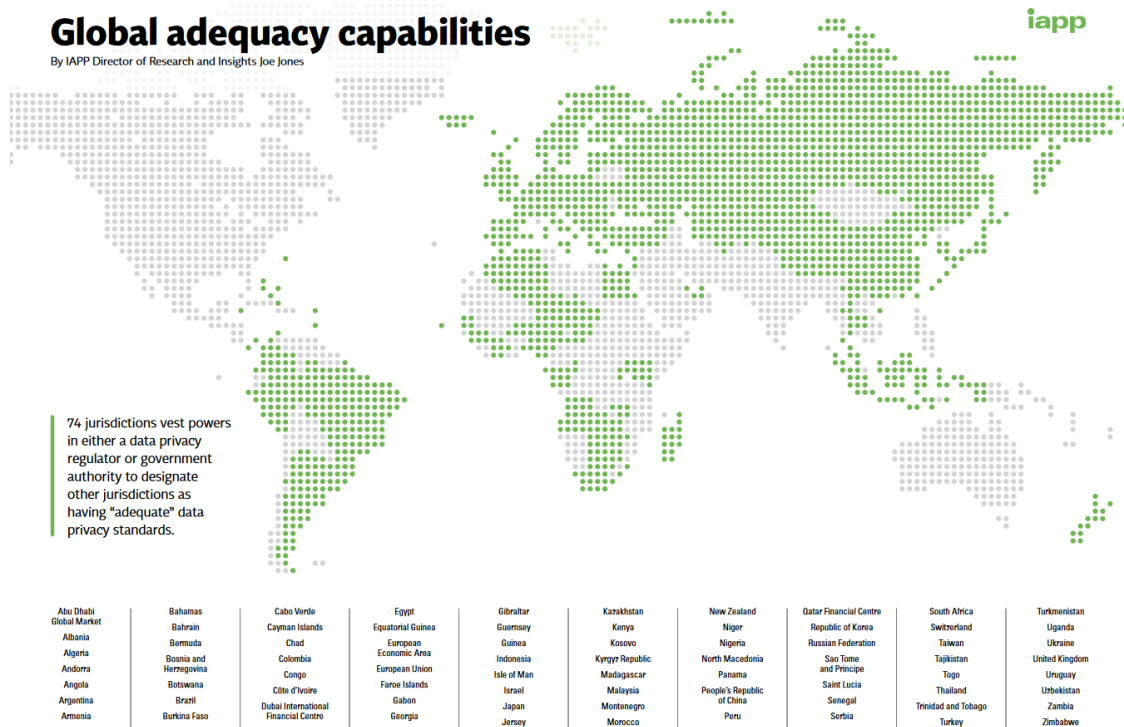
²⁵⁰⁸ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). P. 20.

²⁵⁰⁹ See Chapter XII, Section III.2.

²⁵¹⁰ See Chapter IX, Section III.1.4.1.

Global adequacy capabilities

By IAPP Director of Research and Insights Joe Jones



Source: IAPP, "Infographic: Global adequacy capabilities"²⁵¹¹

An "adequacy light"²⁵¹² option could also be possible. Both Convention 108+ and GDPR require appropriate safeguards when personal data are transferred to a country, non-signatory to the respective Regulation, and to establish one or more SAs for ensuring compliance with its provisions. This could then lead the Commission to expedite the process of assessing a country's level of data protection by considering Parties to the intervention as having an essentially equivalent level of protection. We are of the opinion that the search for and examination of an essentially equivalent level of protection should also take into account treaties whose contracting Parties are States that impose obligations on themselves. Nevertheless, Parties to the intervention – based on those elements aligned with the GDPR – cannot automatically receive an adequacy status, but rather that these countries are candidates with a good baseline.

If the recipient country is not deemed adequate, personal data should still be possible to be transferred under appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. In the case of a TIA, the transfer could then still be made subject to the condition that the data exporter demonstrates the implementation of these safeguards and continuously monitors them to ensure that personal data in the recipient country are treated in the same way as they would be in the exporting country.

These safeguards in the intervention are to be oriented to GDPR and PIPL, since both have similar content, as noted above²⁵¹³; approved CoC and BCR could also to be included, although PIPL does not regulate them. Since the Commission's SDPC were not objected to in *Schrems II* after analysis by the Advocate General, they could serve as a practical part or annex to an intervention to regulate the transfer and in particular

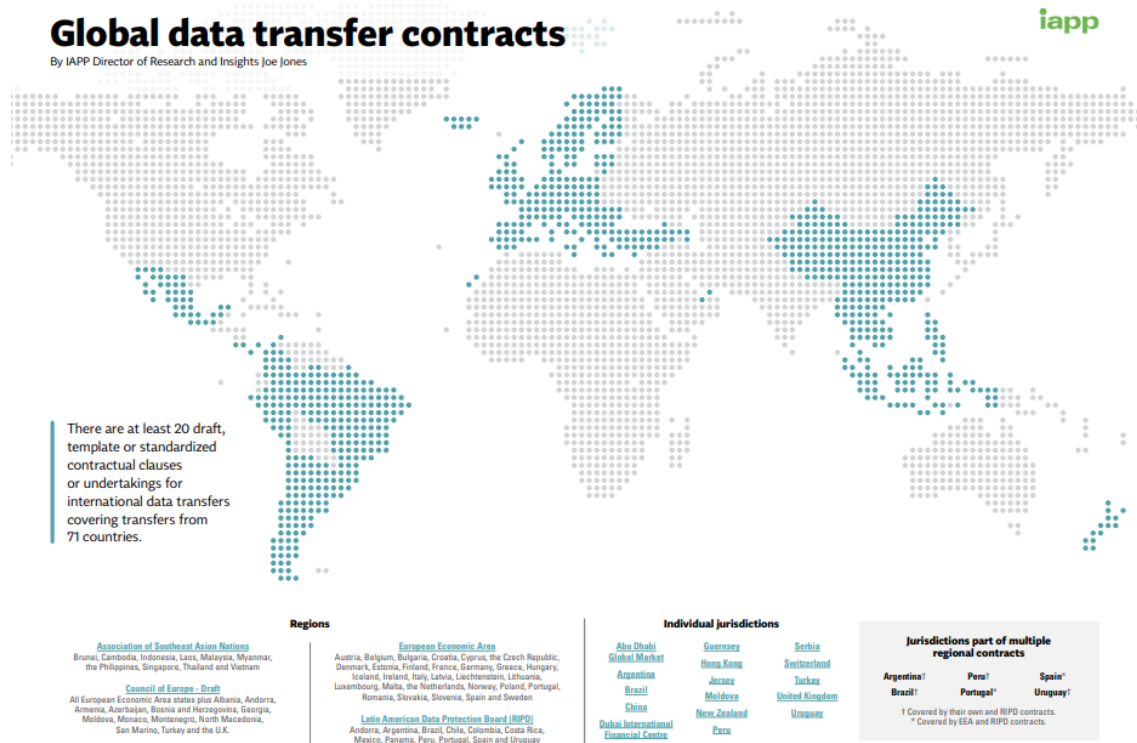
²⁵¹¹ IAPP. (April 2023). *Infographic: Global adequacy capabilities*.

https://iapp.org/media/pdf/resource_center/global_adequacy_capabilities.pdf.

²⁵¹² See Chapter XII, Section II.

²⁵¹³ Chapter IX, Section III.1.4.1.

the onward transfer for companies in a comprehensible manner, in the sense of a practical aid or even in the ruleset part of the intervention. This is supported by the fact that the recognition of this transfer mechanism is increasing:



Source: IAPP, “Infographic: Global data transfer contracts”²⁵¹⁴

We therefore see it as undisputable that the intervention should contain such model clauses or standardized contractual clauses. Nevertheless, the use of such clauses in the intervention would again have to take GATS²⁵¹⁵ into account for the “line between data protection and data protectionism according to WTO law”²⁵¹⁶. It is also necessary to note that recognition of adequate protection of personal data in countries outside the scope of the intervention - similar to an adequacy decision of the Commission - would be an easier way for SMEs to achieve a legitimate TFPD than SDPC. Alex Greenstein, Director of the EU-US DPF at US Department of Commerce and head of the Privacy Shield for 4 years drew this comparison between SDPC and the EU-US DPF by noting that relying on the EU-US DPF

is a more affordable and I guess I would say approachable transfer mechanism. That’s why it was so popular with small and medium enterprises. Standard Contractual Clauses are definitely important, but they definitely skew towards more larger and more sophisticated companies, as around 75% of the Privacy Shield were SME companies.²⁵¹⁷

²⁵¹⁴ IAPP. (April 2023). *Infographic: Global data transfer contracts*. https://iapp.org/media/pdf/resource_center/global_data_transfer_contracts.pdf. // IAPP also found that that SDPC are used by nearly all (94%) of the 473 surveys that were completed, see Chapter IX, Section II.3.

²⁵¹⁵ See Chapter V, Section III.

²⁵¹⁶ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 425.

²⁵¹⁷ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

Naef criticized in 2023 “the EU model data flow clauses [SDPC], which the European Commission endorsed as a model for future negotiations of EU trade agreements in 2018, for not committing to the free flow of personal data across borders and refusing to establish regulatory cooperation in the field of data protection”²⁵¹⁸.

He proposed four new designs for SDPC that

respect the primacy of the right to continuous protection of personal data in Article 8 CFR while still entailing a commitment to the free flow of personal data across borders and regulatory cooperation between the contracting parties in the field of data protection. The four designs further the opportunity to reach greater convergence for high data protection standards on the international plane.²⁵¹⁹ [...]

The first design combines a data flow obligation with a general data protection exception. The second design uses a more specific adequacy exception. The disadvantage of these designs is that the justification for a restriction on cross-border flows of personal data lies with the defendant. The EU would have to prove that a measure is taken for the protection of personal data that is transferred to the contracting party (in case of the first design) or that the level of protection for personal data in the contracting party is not adequate (in case of the second design). The third design combines a data flow obligation with an adequacy condition. The parties allow the cross-border transfer of personal data in cases in which the level of protection for the transferred personal data is adequate. The advantage of this design is that the defendant does not bear the burden of proof because the criterion of an adequate level of protection is not integrated as an exception. However, the term “adequate level of protection” might have a different interpretation in trade agreements than in EU law based on interpretations according to the VCLT. This could provoke problems with the right to continuous protection for personal data in Article 8 CFR. A footnote referring to an autonomous definition of the term could prevent such problems. Another solution could be a provision on cooperation that establishes a dialogue on adequate protection for personal data. The documentation of that dialogue could be used as supplementary means of interpretation according to Article 32 VCLT. The fourth design for a data flow clause is the same as the third design with regards to containing an adequacy obligation and an adequacy condition, but it also has a separate chapter on data protection. The advantage of the fourth design over the third design is that the trade agreement itself provides the basis for an adequate level of protection for personal data.²⁵²⁰

Since we follow the approach of requiring at least an adequacy condition, only Naef’s designs number 3 and number 4 should be considered for the intervention. The interpretation of “adequacy” would not apply if the parties to the intervention could agree on principles and essential guarantees.

The following table shows a comparison of the most important Model Clauses:²⁵²¹

²⁵¹⁸ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 425.

²⁵¹⁹ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 425.

²⁵²⁰ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 415.

²⁵²¹ This table is based on: IAPP. (June 2023). *A practical comparison of the EU, China and ASEAN standard contractual clauses*. <https://iapp.org/resources/article/a-practical-comparison-of-the-eu-china-and-asean-standard-contractual-clauses/#sccs>. We improved it and added the CoE MCC.

Topic Applicability	Key features 1. Access to personal data from another jurisdiction could constitute a transfer.	EU SDPC • Under the GDPR, the concept of "transfer" is broad, as it also applies in the case of remote access to personal data.	CoE MCC • The disclosure or making available of Personal data to a recipient subject to the jurisdiction of a country that is a Non-Party to the Convention.	PRC Standard Contract • Although the term "export" is not clearly defined in PIPL, certain guidelines issued by the authorities suggest the following circumstances will be deemed data transfers: o A controller transfers the data collected and generated in its domestic operations offshore. o A controller stores the data collected and generated in its domestic operations offshore. o The data collected and generated by the controller is stored within China, whereby offshore organizations or individuals may access, retrieve, download or extract it.	ASEAN MCC • Although "transfer" is not expressly defined in the ASEAN MCCs, the illustrations provided in the framework suggest access to personal data from a third jurisdiction could constitute a transfer. • The ASEAN MCCs are a voluntary mechanism available to any organization within the ASEAN transferring personal data to another organization in a different ASEAN country. The MCC provisions are modular, meaning they can be adapted at will, so long as the data exporter and importer adhere to applicable data protection laws including any transfer requirements and/or restrictions imposed upon them in their own territories.
	2. Availability to intragroup transfers, as well as to transfers to external parties.	• Controllers and processors can apply SDPCs to transfer data to third parties as well as in intragroup scenarios	• Available to the Data importer and Data exporter signatories to these Clauses • Also to a Non-Party, which is a State that has not ratified the Convention or where it is not yet in force.	• The PRC Standard Contract can apply to intragroup transfers as well as transfers to third parties.	• The ASEAN MCCs can apply to intragroup transfers, as well as transfers to third parties.
	3. Standards contracts are one among many available legal transfer mechanisms.	• The SDPCs are one of the legal mechanisms available under the GDPR that parties may rely upon to ensure the lawful transfer of personal data to a third country that does not provide adequate levels of personal data protection compared to the EU framework. Generally, SDPCs are available to all controllers and processors who wish to sign and implement them, provided they can adhere to the provisions in practice.	• The CoE MCC are the newest transfer mechanism besides the law of that State or international organization, including the applicable international treaties or agreements; or ad hoc or approved standardized safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing" (Arts. 14(3)(a) and Art. 14(3)(b) Convention 108+).	• The PRC Standard Contract is one of the legal mechanisms available under the PIPL that parties may rely upon to transfer personal data originating from China to a third country, provided that the following criteria are met. To rely on the PRC Standard Contract for personal data export activities, a controller must not fall under Art. 38(1) PIPL. Otherwise, the controller will be subject to the security assessment organized by the government authority.	• The ASEAN MCCs can be adapted and used for data transfers within the ASEAN. This would satisfy any member state laws that recognize a data transfer agreement or contract as one of the ways an outbound transfer can be lawfully carried out. However, where a member state has requirements that contradict the MCCs, for instance if there is data localization which requires data is only processed and stored in-territory, the local law requirement will prevail.
Topic Fixed form	Key features 1. No changes are allowed/changes are allowed.	EU SDPC • The text of the SDPCs is not amendable, except to select modules and/or specific options offered in the text, complete the text where necessary, fill in the annexes, or add additional safeguards that increase the level of protection for the data. Optional elements of the SDPCs include a docking clause that allows additional parties to join the contract in the future or an additional redress clause that allows data subjects to lodge complaints with an independent dispute resolution body at no cost. • The parties can incorporate the SDPCs into broader commercial contracts so long as the other contractual provisions do not contradict the provisions in the SDPCs, either directly or indirectly, or prejudice the rights of data subjects.	CoE MCC • These Clauses set out appropriate safeguards, including obligations for Controllers, enforceable Data subject rights and effective legal remedies, pursuant to Articles 14(2) and 14(3)(b) of the Convention, provided they are not modified, except to add or update information in the Annexes. • These Clauses are without prejudice to obligations to which the Data exporter is subject by virtue of the Applicable law.	PRC Standard Contract • The text of the PRC Standard Contract is not amendable and must be strictly followed, though the parties will be able to fill in the applicable blanks and select the dispute resolution mechanism. Additional provisions, that do not contradict the PRC Standard Contract, agreed between the parties can be added to the PRC Standard Contract in a separate appendix. • The PRC Standard Contract is a standalone contract. The parties will be able to refer to the commercial contract in the preamble.	ASEAN MCC • There are additional optional modules offered in the MCCs which parties can choose to include in their final executed agreement.
	2. A description of the personal data transfers must be provided/or not.	• Details about the transfer must be provided, including the categories of personal data, categories of data subjects, retention periods, as well as, where applicable, the list of subprocessors and the supplementary technical and organizational measures identified.	• Similar to the EU SDPC.	• Details about the export need to be included, including the purpose and method of export, the type and volume of the personal data being exported, the details on onward transfers by the offshore recipient, the transmission method, the offshore retention period, and the location of storage; the security and organizational measures to be taken by the offshore recipient; and the point of contact of the offshore recipient to respond to data subject inquiries.	
Topic Modules	Key features A modular approach is accepted/promoted.	EU SDPC • SDPCs are designed for four possible transfer scenarios: controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller.	CoE MCC • CoE MCCs are limited to one scenario for both controllers and processors. Interestingly, the draft version of the CoE MCC states "Controller to Controller" as the only scenario.	PRC Standard Contract • The PRC Standard Contract applies to all personal data export activities by controllers only. Unlike the EU SDPCs, it does not differentiate controller-to-controller or controller-to-processor transfers, nor does it apply to data transfers by a processor.	ASEAN MCC • The ASEAN MCCs are designed for two possible scenarios: C2C and C2P transfers.

Topic	Key features	EU SDPC	CoE MCC	PRC Standard Contract	ASEAN MCC
Data transfer and personal information protection impact assessments	1. A risk assessment must be conducted prior to the transfer.	<ul style="list-style-type: none"> A TIA helps ensure SDPCs will provide appropriate safeguards and effective and enforceable rights for individuals. It involves a detailed assessment of the laws and practices of the third country of destination. As part of the DTIA, parties should assess the risks related to the transfer, such as the risk of public authorities accessing personal data, as well as the possibility for data subjects to effectively enforce their rights. If the assessment determines the personal data is insufficiently protected by the safeguards provided under the SDPCs, then supplementary measures should be adopted to address the deficiencies identified. 	<ul style="list-style-type: none"> The Data exporter warrants that it has used reasonable efforts to determine that the Data importer is able, in particular, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses. 	<ul style="list-style-type: none"> As required by the PIPL, a PIPIA is the precondition of carrying out any personal data export activities. A PIPIA on data exports shall include: <ul style="list-style-type: none"> The legitimacy and necessity of the purpose, scope and method of the processing by the controller and the offshore recipient. The volume, scope, type and sensitivity of the personal data being exported, and the risks associated with the export on the data subjects' rights and interests. The undertakings of the offshore recipient, and the effectiveness of the technical and organizational measures taken by the offshore recipient in terms of safeguarding the personal data. The risk of a data breach after the export of personal data, and whether an effective mechanism has been established to protect the data subjects' rights and interests. The legislative environment of foreign jurisdictions where the offshore recipient is located, and how it may impact the performance of the PRC Standard Contract. Other matters that may influence the security of personal data in the context of a data export. 	<ul style="list-style-type: none"> Silent on this key feature.
	2. The assessment includes an evaluation of the third country's legal framework.	<ul style="list-style-type: none"> Data exporters are required to assess if there is anything in the law and/or practices of a third country that may impinge on the effectiveness of the appropriate safeguards being relied upon and in the context of the specific transfer. 	<ul style="list-style-type: none"> Local laws and practices affecting compliance with the Clauses are addresses in Art. 22 of the CoE MCC. 	<ul style="list-style-type: none"> Under the PRC Standard Contract, both the controller and the offshore recipient are obligated to evaluate whether the legislative environment of the foreign jurisdiction where the offshore recipient is located may impair the offshore recipient's performance of the PRC Standard Contract. The PRC Standard Contract also sets forth the detailed aspects to be considered for the evaluation, including the export details, prior experience of the offshore recipient, and policies and legislations of the foreign jurisdiction. The assessment on foreign jurisdictions should be included in the PIPIA report. 	<ul style="list-style-type: none"> Silent on this key feature.
	3. The assessment should be transfer specific and consider whether the transfer is necessary.	<ul style="list-style-type: none"> The TIA should be transfer-specific and consider whether the transfer meets the necessity test. The SDPCs require the parties to consider the specific circumstances of the transfer. Examples include the length of the processing chain, the number of actors involved, the transmission channels used, intended onward transfers, and the type of recipient. 	<ul style="list-style-type: none"> The Data importer guarantees that it has carefully considered the impact the intended Processing might have on the rights and fundamental freedoms of Data subjects prior to the commencement of such Processing, according to the circumstances of the specific Transfer, and has taken the necessary and appropriate technical and organisational measures to comply with these Clauses, and to demonstrate such compliance to the competent SAS. 	<ul style="list-style-type: none"> A critical part of the PIPIA is to justify and demonstrate in the report the necessity of the personal data export, which is the fundamental requirement of exporting personal data under the PIPL. The factors to consider typically include the nature of the data subjects, the types of data being exported and the purpose of the export. 	<ul style="list-style-type: none"> Silent on this key feature.
	4. A risk-based approach is adopted generally.	<ul style="list-style-type: none"> Even if in a footnote, the SDPCs allow data exporters to take a risk-based approach when conducting the TIA. When assessing the impact of the laws and practices on compliance with the SDPCs, the data exporter can take into account "relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time frame." However, these elements should be part of an overall assessment and, when they are used to justify the transfer, the conclusion should be supported by other relevant, objective elements. 	<ul style="list-style-type: none"> The Data importer and, during transmission, also the Data exporter shall implement appropriate security measures, both of a technical and organisational nature, for each Processing, in particular to protect against the risk of Data breaches. Technical and organizational measures are set out in Annex 3. 	<ul style="list-style-type: none"> The offshore recipient's prior experience with similar exports or requests from public authorities to access personal data should be taken into account during the evaluation discussed in the second point above. 	<ul style="list-style-type: none"> Silent on this key feature.
	5. Additional measures may have to be included to ensure an adequate protection.	<ul style="list-style-type: none"> If a third country's legislation cannot guarantee a level of protection that is equivalent to the one provided under the EU framework, then technical, contractual, i.e., additional clauses, and organizational measures, i.e., specific policies and procedures, can also be put in place to address deficiencies identified in the TIA. 	<ul style="list-style-type: none"> The Data importer and, during transmission, also the Data exporter shall implement appropriate security measures, both of a technical and organisational nature, for each Processing, in particular to protect against the risk of Data breaches. Technical and organizational measures are set out in Annex 3. 	<ul style="list-style-type: none"> The specific technical measures to be taken by the offshore recipient should be added to the PRC Standard Contract. The controller has the obligation to use reasonable efforts to ensure those measures have been taken by the offshore recipient. 	<ul style="list-style-type: none"> The ASEAN MCCs provide that the data exporter must ensure the importer has reasonable and appropriate technical, administrative, operational and physical measures in place that are consistent with applicable data protection laws. However there are no requirements for parties to assess and put these measures in place over and above what the contractual language stipulates.
	6. Monitoring obligations apply.	<ul style="list-style-type: none"> The SDPCs do not contain specific provisions for when a TIA must be redone. However, in its January 2020 recommendations, the European Data Protection Board stated data exporters must monitor, on an ongoing basis, developments in the third country to which they have transferred personal data when such developments could affect the assessments they made and the decisions they took. 	<ul style="list-style-type: none"> The Data importer shall review the legality of any request for disclosure, in particular whether it is within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. 	<ul style="list-style-type: none"> Unlike the EU SDPC, the PRC Standard Contract contains specific requirements on when a PIPIA must be redone. The parties are required to redo the PIPIA, amend or re-sign the PRC Standard Contract and make a new filing if there is: <ul style="list-style-type: none"> Any change in the purpose, scope or types of personal data being exported; any change of the method of the export or the location of storage; or any change in the offshore recipient's usage, method of processing or retention period. Any change in the foreign legislation or policy that may impair the rights and interests of the data subjects. 	<ul style="list-style-type: none"> Silent on this key feature.

Topic	Key features	EU SDPC	CoE MCC	PRC Standard Contract	ASEAN MCC
Data breaches	Do the standards clauses require the reporting of personal data breaches?	<ul style="list-style-type: none"> The SDPCs require data importers to take measures to address data breaches and mitigate their adverse effects. The SDPCs also require data importers to report data breaches, with varying reporting obligations depending on the module and the level of risk arising from the breach. In the C2C module, the data importer must notify the data exporter and the competent SA if the breach is likely to result in a risk to the rights and freedoms of individuals as well as the data subjects if the likelihood of such risk is high. In the C2P and processor-to-processor modules, the data importer must notify the data exporter (and its data controller in the P2P module, if feasible), and assist the data exporter in complying with its own notification obligations. In the P2C module, when a data breach happens at the data exporter's level, it is the data exporter who must notify and assist the data importer. 	<ul style="list-style-type: none"> Similar to the EU SDPC. 	<ul style="list-style-type: none"> In case of data breaches, the PRC Standard Contract requires the offshore recipient to promptly take remedial actions and mitigate the impact on the data subjects; notify the breaches to the controller and the supervising authority, and, if required by the law, the data subjects directly; and keep records on the breach and the remedial actions. The notice to the controller and supervising authority should include: <ul style="list-style-type: none"> The types of personal data affected by the breach, the cause, and potential consequences and impact. The remedial actions being taken. The remedial actions that could be taken by the controller to mitigate the loss. The contact of the person or team responsible for dealing with the breach. In cases where the offshore recipient is an entrusted party, i.e., similar to C2P transfers under the GDPR, the notices to data subjects must be delivered by the controller. 	<ul style="list-style-type: none"> Yes, but through an optional module only. The ASEAN MCCs require the data importer to notify the data exporter of any data breaches it becomes aware of, and parties have the option to determine the period in which this is done, for instance, without undue delay or within a reasonable time specified by the parties.
Onward transfers	Specific conditions must be met for onward transfers.	<ul style="list-style-type: none"> An onward transfer may only take place if the data importer meets certain conditions, which vary depending on the module. For instance, specific grounds for the transfer should be identified. Grounds for the C2C, C2P and P2P modules include, for example) the third-party being bound by the SDPCs;) the third country benefiting from an adequacy decision; or the onward transfer being necessary for specific reasons, e.g., to establish, exercise or defend legal claims, to protect the vital interests of individuals, etc. Additional grounds are available only for the C2C module, such as obtaining the explicit consent of the data subject. 	<ul style="list-style-type: none"> The Data importer shall not onward transfer unless: <ul style="list-style-type: none"> the law of the Third party's jurisdiction, including its international commitments under applicable international treaties or agreements, ensures an appropriate level of protection; the Third party enters into a legally binding and enforceable instrument with the Data importer ensuring the same level of data protection as under the CoE MCC, and the Data importer provides a copy of these safeguards to the Data exporter; the Onward transfer it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings in a particular case; the Onward transfer it is necessary in a specific case in order to protect the vital interests of the Data subject or of another natural person. Any Onward transfer is subject to compliance by the Data importer with safeguards under these Clauses, in particular as regards purpose limitation. 	<ul style="list-style-type: none"> An onward transfer may only take place if all the following requirements are met. Necessity in terms of business, sufficient notice to the data subjects on the onward transfers, to the extent required by the law, proper consent from the data subjects if the processing is based on consent, written agreement with the third-party recipient, ensuring that such recipient could meet the standard of protection required by the PRC laws, data subjects have the right to request a copy of the agreement with the third-party recipient. 	<ul style="list-style-type: none"> The ASEAN MCCs provide a module to address any onward transfers. The data importer must only carry out an onward transfer after notifying the data exporter of this in writing and giving the exporter a reasonable opportunity to object. The importer also must ensure any third-party recipient is bound by the same obligations as those that the data importer owes to the data exporter.
Suspension of transfers	The standards provide for the possibility/obligation to suspend the transfer in case the protection afforded to personal data is not effective.	<ul style="list-style-type: none"> Under the SDPCs, the data exporter must suspend the data transfers if the data importer breaches or is unable to comply with its obligations under the SDPCs, or if the data exporter is instructed to do so by the competent SA or the data controller, in the P2P module. In the event of suspension, the data exporter may be entitled to terminate the contract with the data importer. To do so, one of the termination grounds must be present, such as if the suspension exceeds a reasonable time, one month in any event and if the data importer is in substantial or persistent breach. 	<ul style="list-style-type: none"> The Data importer accepts that the SA in order to protect the rights and fundamental freedoms of data subjects, is entitled to prohibit transfers, suspend them or subject them to conditions notably in cases where the Clauses are not complied with. The Data exporter shall suspend the Transfer if it considers that no appropriate safeguards for such Transfer can be ensured, or if instructed by the competent SA to do so. 	<ul style="list-style-type: none"> Under the PRC Standard Contract, the controller may suspend the export of personal data if the offshore recipient violates its contractual obligations under the PRC Standard Contract or if a change in policy and legislation of the jurisdiction where the offshore recipient is located results in the recipient's failure in performance of the PRC Standard Contract. In addition, if the suspension lasts for more than one month, the controller has the right to terminate the PRC Standard Contract. 	<ul style="list-style-type: none"> The ASEAN MCCs stipulate that if the data importer is in breach of its obligations, either under the MCCs or applicable law, then the data exporter is entitled to temporarily suspend the transfer of data until the breach is repaired or processing under the agreement is terminated.
Retention requirements		<ul style="list-style-type: none"> There is no requirement to file the SDPCs nor to retain the TIA for a specific amount of time. 	<ul style="list-style-type: none"> Each Party shall be able to demonstrate compliance with its obligations under these Clauses. To this end, it shall keep appropriate documentation of the Processing activities carried out under its responsibility. Each Party shall make such documentation available to the competent SAs on request. 	<ul style="list-style-type: none"> The executed PRC Standard Contract and the PIPIA report on the personal data export must be filed with the provincial Cyberspace Administration of China within 10 working days after the PRC Standard Contract takes effect. All documents must be written in Chinese. The PIPIA report must be retained for at least three years. Note that the measures on PRC Standard Contract will take effect 1 June, and a six-month grace period is granted to existing export activities. 	<ul style="list-style-type: none"> There is no requirement to register the ASEAN MCCs, although, in principle, if a data exporter is required under local law to file a transfer agreement with a local authority, it can do so using the MCCs in their executed form.
Governing law and forum	<p>1. Obligation to identify a local governing law.</p> <p>2. Obligations in relation to competent forum.</p>	<ul style="list-style-type: none"> The governing law must allow for third-party beneficiary rights and, in most cases, it must be the national law of a EEA country. The parties can only specify the national law of an EEA or non-EEA country in the P2C module. Similar rules apply when choosing the competent forum, i.e., the obligation to identify the courts of an EEA country in most cases. However, a data subject may also bring legal proceedings before the courts of the EEA country of their habitual residence. 	<ul style="list-style-type: none"> Domestic rules for the protection of personal data applicable in the jurisdiction of the data exporter. Parties are free to choose the forum of dispute resolution. Data subjects may also bring legal proceedings against the Data exporter and/or Data importer before the courts of the country in which they have their habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts. 	<ul style="list-style-type: none"> The PRC Standard Contract must be governed by the PRC laws. The parties to the PRC Standard Contract may choose a Chinese court or an international arbitration tribunal under the New York Convention as the mechanism of dispute resolution. Data subjects, as the third-party beneficiaries, may bring legal claims in Chinese courts. 	<ul style="list-style-type: none"> Parties are free to choose the governing law of the ASEAN MCCs, among the 10 member states. Parties are free to choose the forum of dispute resolution.

Topic	Key features	EU SDPC	CoE MCC	PRC Standard Contract	ASEAN MCC
Supervisory authority	Organizations will need to work with local supervision (with some exceptions).	<ul style="list-style-type: none"> In most cases, the SDPCs require the identification of an EEA data protection authority, determined based on the territorial scope of the data exporter. In the C2C, C2P and P2P modules, the parties must designate the SA competent for the data exporter's compliance with the GDPR, if the exporter is established in the EEA; the SA of the representative's establishment, if the data exporter is not established in the EEA but has appointed a representative; or the SA of one of the EEA countries where the data subjects' data is transferred are located, if the data exporter is not established in the EEA and has not appointed a representative. There is no requirement to identify an EEA SA for the P2C module. The SDPCs also allow data subjects to lodge a complaint with the EEA SA in the country of their habitual residence or place of work. 	<ul style="list-style-type: none"> SA is defined as one or more authorities responsible for ensuring compliance with the provisions of the Convention as incorporated by the Applicable law. The Data exporter shall cooperate with and provide reasonable assistance to the Data importer if that is necessary to allow [to enable?] the Data importer to comply with its obligations this Section. Any dispute, controversy or claim between the Parties arising under, out of or relating to these Clauses including, without limitation, their formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall be referred to and finally determined by arbitration in accordance with the WIPO Arbitration Rules 	<ul style="list-style-type: none"> Under the PRC Standard Contract, the SA refers to the provisional and state CAC. Notably, by signing the PRC Standard Contract, the offshore recipient accepts the supervision and administration of the CAC, including, but not limited to, answering inquiries, cooperating with inspections, complying with measures taken or decisions made by the CAC, and providing written certificates as requested. 	<ul style="list-style-type: none"> The ASEAN MCCs are silent on any SA, as they are voluntary in nature and local data protection laws will continue to apply to the respective parties.

Here, too, the intervention should harmonize the key features within this table – oriented to the objectives –, if it includes Model Clauses in the standard text, which we are in favor of. Otherwise, the worldwide increase of such clauses (see graphic on “Global data transfer contracts” above), in combination with aforementioned divergent designs, would lead to a high challenge of coping with unharmonized standard contracts, as rightly stated by the IAPP:

With the development of multiple standards, hoping for one single set is probably a pipe dream, and one that might even not be fully functional, as it will likely lead to a stricter-rule approach). This raises questions about what, if anything, can be done to achieve a greater level of interoperability. Policymakers play a pivotal role in working toward mutual recognition of the currently fragmented patchwork of standard contracts that underpin global data transfers. In their recently published first-of-its-kind guide²⁵²² identifying the similarities and differences between the ASEAN MCCs and the EU SCCs, the European Commission and the ASEAN explained their objective was to aid companies in meeting requirements under both sets of contractual clauses, as well as their data protection laws, more broadly. Hopefully, this will be the first of many guides that offer an approach for interoperability between two otherwise distinct sets of contractual clauses. Without any consensus, multinational corporations with business or operations that straddle more than one of these blocs would need to draft intragroup agreements that include multiple sets of SCCs, built as appendices and with particular attention paid to hierarchy clauses.²⁵²³

A new regulatory instrument would also have to take better account of the duties²⁵²⁴ to be fulfilled by the SAs of the Parties to this new agreement. Naef proposed that

first, the different supervisory authorities must adopt the same policy for data transfers to a specific third country (consistency among the different supervisory authorities). Second, every supervisory authority must adopt the same policy for data transfers to all third countries that pose similar threats to fundamental rights in order not to discriminate against certain countries”²⁵²⁵.

Both should be specified in the intervention. However, the intervention would have to avoid that the affected SAs of the Parties struggle to fulfill their new duties, as many SAs

²⁵²² ASEAN and European Commission. *Joint guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*. <https://asean.org/wp-content/uploads/2023/05/The-Joint-Guide-to-ASEAN-Model-Contractual-Clauses-and-EU-Standard-Contractual-Clauses.pdf>, (2023).

²⁵²³ IAPP. (June 2023). *A practical comparison of the EU, China and ASEAN standard contractual clauses*.

<https://iapp.org/resources/article/a-practical-comparison-of-the-eu-china-and-asean-standard-contractual-clauses/#sccs>.

²⁵²⁴ Chapter IX, Section 1.1.4.

²⁵²⁵ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 426.

are – and this only with regard to the GDPR – already underfunded and understaffed.²⁵²⁶ A comprehensive and coordinated course of action would then be required. Naef proposed therefore the consistency mechanism in Article 64 GDPR as a remedy, although others may be necessary as well.²⁵²⁷

Even when there is no TIA, no adequacy decision and no appropriate safeguards in place, the intervention could still allow such transfers in scenarios with external relationship under certain derogations. The OECD already gave a good outline for these derogations:

Contractual arrangements or other fairly standard conditions such as: that the data subject's consent is obtained; that a data transfer is required to fulfil a contractual need; that a data transfer is in the public interest; that a data transfer is needed for legal cooperation; or that a data transfer is deemed necessary for the protection of the data subject's vital interests, to name the most common.²⁵²⁸

The GDPR identifies clearer derogations in its Chapter V, while Art. 38(4) PIPL leaves room for interpretation. In that aspect, intervention should therefore be oriented towards the OECD Guidelines 2013 and the GDPR.

In TFPD scenarios with external relationship, one could even resort to the “strictest” mechanism, which consists of an ad hoc authorization of an authority. We have to annotate again the difference to “ad hoc clauses” as recognized safeguards; the latter are a set of clauses for TFPD, which require prior approval by a DPA, or contracts negotiated between the data exporter and the data importer, subject to approval from the competent DPA. In the strictest mechanism, however, not only certain clauses are examined, but an authorization then refers to all transfers with external relationship, either generally all, those of a specific sector, or those of a specific data type. Those would then be subjected to a review by a relevant authority, in our case the UN HRC. Such a mechanism could, however, be too restrictive and could significantly complicate TFPD between in-scope countries and out-of-scope countries. In addition, the administrative burden for the UN HRC could be too high due to case-by-case reviews. We therefore reject such a mechanism. Since this mechanism originates from Art. 38(1) PIPL and has only recently been detailed in China through the PRC Security Assessment Measures, opposition from China to an intervention without such a mechanism is to be expected. To reach consensus, it could be conceivable to include criteria for a CAC-led assessment in an intervention, to subsume it under the rationale “national security / public order / sovereignty”, and thereby to allow data flow restrictions for such data types. Quantitatively, one could determine a “cumulative transfer of personal data of 100,000 or more individuals or sensitive personal data of Mr or more individuals”; qualitatively, one could determine personal data processed by OCII. In any case, the vague provision in PIPL that requires a CAC-led assessment also for “other circumstances to be specified by the CAC” should be rejected.

In all TFPD scenarios, both in-scope transfers and such with external relationship, data flow restrictions should be “strictly necessary”. This criterion originates from Art. 52(1) Charter and Art. 29(2) UDHR and was reaffirmed by both the CJEU²⁵²⁹ and G7. Moreover, for both transfer scenarios, processing activities in the domain of “national

²⁵²⁶ Clark, S. [Sam]. (6 August 2020). *GDR analysis: European regulators buckling under Schrems pressure*. <https://globaldatareview.com/article/gdr-analysis-european-regulators-buckling-under-schrems-pressure>.

²⁵²⁷ Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer. P. 427.

²⁵²⁸ OECD. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, (21 December 2018). Para. 33.

²⁵²⁹ CJEU. Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Other*, Case C-623/17, ECLI:EU:C:2020:790. Para. 68.

security / public order / sovereignty” or “universal bads” recognized by international law, as well as the flow restrictions based on such rationales, should be subject to an independent and effective review and supervision.

Whenever permitted derogations strengthen the cybersovereignty of one Party to the possible detriment of another Party, the system of reciprocity becomes relevant. The intervention could ensure that criteria for establishing regulatory sovereignty at the international level become criteria for all States, i.e., that they can develop into generally accepted principles. If a State claims regulatory sovereignty for itself under certain circumstances, it cannot deny it to other States in comparable circumstances.

2. Non-legislative elements

The goal of this thesis is to create a single regulatory intervention that addresses all legal aspects of a TFPD; the creation of other measures alongside such an intervention is generally not intended. Such “other measures” are important in this thesis, however, if they can only be solved via the specific objective of cooperation.²⁵³⁰ In line with the blended governance approach²⁵³¹, the intervention could also have to include measures that do not comprise legislative elements but also non-legislative elements.

For in-scope scenarios, it is not as relevant as for scenarios with external relationship to establish cooperation, since a uniform level of protection is guaranteed by the transfer mechanism, principles, essential guarantees, and maturity level, which are uniform on a consensus basis and integrated in the intervention. However, to integrate the idea of “data flows where there is trust”²⁵³² for the success of an intervention, more is needed than uniform rules, even for in-scope scenarios. As the WEF noted, “the wider societal challenge does not end there: technical infrastructure is needed to share data and ensure its cross-system usage. Even more broadly, people must be able to make sense of the data and apply it in new contexts”²⁵³³. Aaronson also noted that “policy makers should focus first on creating an effective enabling environment for data, then build trust in that new economy by empowering people around the world to control their data.”²⁵³⁴ Stakeholders expressed concerns “about the lack of interoperability and openness of these systems, especially for developing countries outside the relevant regional and plurilateral forums. Public-private dialogue among responsible jurisdictions and stakeholders could help alignment and transparency.”²⁵³⁵ These concerns could be addressed through trust, meeting the specific objective “trust”²⁵³⁶, and multi-stakeholder participation. Also, in-scope and out-of-scope regulators could be supported by creating mechanisms that encourage the development and application of common principles and collaboration between them. The intervention could integrate the invitation for non-Members to adhere and to collaborate. To support collaboration, therefore, “different

²⁵³⁰ See Chapter X, Section II.2

²⁵³¹ See Chapter I, Section II.4.

²⁵³² WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 16.

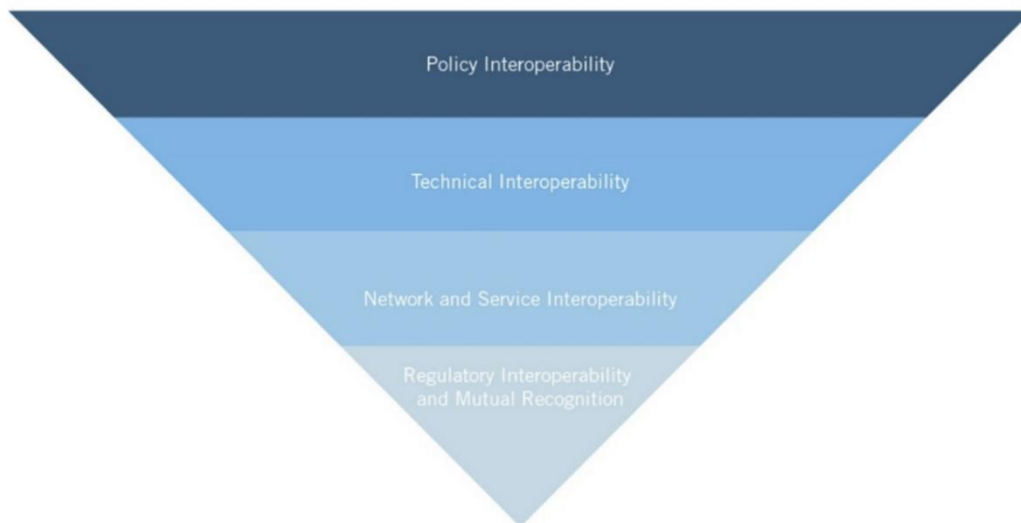
²⁵³³ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 16.

²⁵³⁴ Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>. P. 3–4.

²⁵³⁵ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 17.

²⁵³⁶ Chapter X, Section II.5.

tools at different technological layers and levels of integration²⁵³⁷ could therefore be used which the following graphic correctly divides into different “layers”.



Source: Cory, Nigel / Dascoli, Luke, “The different layers of global digital interoperability”²⁵³⁸

These tools straddle the line between legislative elements and non-legislative elements. For scenarios with external relationship, unilateral or reciprocal adequacy decisions could serve as a tool that “should be encouraged to expedite these decisions and base them on well-defined and transparent criteria according to procedural fairness”²⁵³⁹.

Although the APEC framework does not approach the standards of intervention in its substantive law, it has a strength in elaborating tools for cooperation. In 2016, organizations within APEC started using the so-called “Cross-Referential” document to fulfill both instruments’ qualifications and to enable MNEs satisfy requirements of both instruments for transborder transfers between APEC and EEA countries, and to other countries outside these regions.²⁵⁴⁰ In April 2022, the participating economies declared the “establishment of a Global CBPR Forum to promote interoperability and help bridge different regulatory approaches to data protection and privacy”²⁵⁴¹. The Global CBPR Forum “intends to establish an international certification system based” and “will be independently administered and separate from the APEC Systems”²⁵⁴². Similar to the efforts of the Global CBPR Forum is the EU’s “Coordinated Enforcement Framework”²⁵⁴³. The “coherence procedure”²⁵⁴⁴ from the European framework could also be adopted. The intervention could integrate such a forum at the UN level as well as a cross-referential.

²⁵³⁷ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

²⁵³⁸ Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

²⁵³⁹ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 17.

²⁵⁴⁰ WP29. *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*, WP 212, (27 February 2014).

²⁵⁴¹ USA, Department of Commerce. *Global Cross-Border Privacy Rules Declaration*, <https://www.commerce.gov/global-cross-border-privacy-rules-declaration>, (2022).

²⁵⁴² USA, Department of Commerce. *Global-Cross-Border-Privacy-Rules-Declaration-FAQ*, <https://www.commerce.gov/sites/default/files/2022-04/Global-Cross-Border-Privacy-Rules-Declaration-FAQ.pdf>, (2022).

²⁵⁴³ See Chapter IX, Section I.1.4.

²⁵⁴⁴ See Chapter IX, Section I.1.4.

Among approaches to regulated self-regulation, BCR are particularly conducive to a universal level of data protection, as long as their benefits exceed the costs associated with them; the bureaucratic effort involved in issuing BCR is still high at the present time. The benefits of BCR could be increased if BCR's function was brought closer to that of CoC.

Interoperability with a technical focus could be established through a common infrastructure in the form of "secure data spaces". This could be designed like the "Microsoft German Cloud", which was in operation until the end of 2021. Within this structure, Microsoft continued to be fully responsible for all aspects of the operation and provision of its cloud services, which did not require access to customer data, with no connection or networking of any kind with other (Microsoft) cloud services. If Microsoft wanted to access the "German Cloud", Microsoft had to apply to a data trustee (which could in our case be a UN body) for such access, and the trustee was only authorized under the contract with the customer to grant temporary access in certain cases. The purposes of data access were strictly limited to troubleshooting and maintenance. In the case of a customer's personal data, a differentiation was made between data that was required for billing purposes, for example, and the actual customer data.

PETs could be an obligation in the product development process to program data protection requirements (Privacy by Design). Appropriate programming could be used to ensure that certain data are not generated in the first place or are excluded for a combination with other data for the purpose of creating profiles. A transatlantic consensus could probably be reached on the optimization of consent solutions, since these questions originated in the North American legal area and were early on the US government's agenda.²⁵⁴⁵ On the other hand, there is less international consensus on the question of when certain forms of data processing activities should be prohibited regardless of consent. The Google judgment of the CJEU demonstrated that this can lead to legal friction if a foreign ISP wants to operate in a country with higher data protection standards. Within the UN, such PETs are already acknowledged. The UN Committee of Experts on Big Data and Data Science for Official Statistics "launched a UN PET Lab that has the specific aim to pilot a program that would make international data sharing more secure by using PETs. The UN PET Lab will bring together statistical bodies to collaborate with technology providers that offer PET technologies to test solutions to transfer data across borders compliantly."²⁵⁴⁶

The quality of the consent mechanism could be improved in an intervention. It is difficult for a user (and data subject) to understand what he is giving his consent to, for what purpose the data are collected, processed and forwarded, if and when data are deleted. Where laws prescribe a declaration of consent of the data subject, the goal of "free and informed consent" is often undermined by the fact that a page-length declaration is used in a barely legible typographic design. Normally, the normal user still relies on it and trades possible future disadvantages for immediate use. The factual monopoly of some providers such as Meta is exacerbating this. The intervention could include data protection-friendly default settings, in which the user can explicitly select certain uses of his data instead of having to exclude them (Privacy by Default). Another non-legislative possibility in this respect could be one similar to "Global Privacy Control" (GPC)²⁵⁴⁷,

²⁵⁴⁵ USA, The White House. *Big Data: Seizing opportunities, preserving values*, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, (May 2014). P. 53 ff.

²⁵⁴⁶ OECD. (12 October 2022). *Cross-border Data Flows. Taking Stock of Key Policies and Initiatives*. <https://www.oecd.org/publications/cross-border-data-flows-5031dd97-en.htm>. P. 10.

²⁵⁴⁷ <https://globalprivacycontrol.org/>

which provides a way to opt out at the browser or device level. This would be an improvement over the need to opt out at every site or on every service.

IV. Competent authorities: UN Human Rights Council, International Court of Justice for Cyberspace Affairs

International authorities would have to be selected for different responsibilities, which are consultation and enforcement. This could be one authority competent to develop guidelines and recommendations – similar to WP29 / EDPB –, and a judicial authority which could issue judgments with *erga omnes* effect, with a dispute settlement procedure not depending on the Parties' discretion.²⁵⁴⁸ The question arises as to the need for either the creation of a new organization or extending the mandate of an existing one.

The UN Guidelines were the first global consensus on data protection. In the following development, however, the UN Guidelines have become less important. The repeated requests of the UN General Assembly to Member States to express their views on the definition of key terms related to information security shows the efforts of the UN to a channeling of international discussion and the creation of a uniform conceptual basis, which is indispensable for the success of an international convention. The UN could, beyond their mere communication function, play a role in the development of the intervention. Nevertheless, more possible it seemed three years ago to develop a global UN convention against cybercrime. But, again, the CoE is a step further and has already adopted the CCC. Accordingly, the Secretary General of the CoE proposed to the UN the accession to the CCC instead of the lengthy design of an own Cybercrime Convention by the UN. The international debate focuses, in particular due to the fight against terrorism, still on the issue of the security on the Internet. At the UN, the focus has therefore shifted from data protection to cybercrime. It remains to be seen if the UN organs adheres to this direction.

Nevertheless, we believe that the UN HRC could be the consultative body for the intervention, which also sets and oversees the rules for a “regulatory sandbox / RPS”. Requests to participate in this RPS could then be evaluated by the UN HRC on a case-by-case basis. It could also be the responsibility of the UN HRC to establish a “Joint Oversight Committee” to review the proposals of the intervention and to ensure that the RPS is not used to deviate from or circumvent existing laws, and that it serves as a central point of contact with the authority to engage other authorities as needed. The UN HRC could be assigned to help States transform their national legal frameworks to be conform with the rules of the intervention. A strengthened interoperability with other instruments such as the CBPR, GPEN or the Internet & Jurisdiction Project²⁵⁴⁹ could be seen as an instrument at the border between legislative and non-legislative elements. Activities with these networks could at the same time represent activities to provide mutual legal assistance, reduce administrative burdens for companies in a large and economically important area, and lead to a gradual harmonization of data protection practice. With these networks, MLATs among data protection SAs could be established for the purpose of law enforcement. In our view, the UN HRC could constitute this SA within the framework of the intervention.

²⁵⁴⁸ See Chapter XII, Section IV.

²⁵⁴⁹ The work of the organization has been presented to and recognized by key international processes, including the UN Internet Governance Forum, the UN Secretary-General's High-level Panel on Digital Cooperation, G7, G20 or the Paris Peace Forum, and covered in top media outlets such as The Economist, New York Times, Washington Post, Financial Times, Politico or Fortune. See Internet & Jurisdiction Policy Network. (2023). *Mission*. <https://www.internetjurisdiction.net/about/mission>.

Kuner argued correctly that laws that lack the means to enforce may diminish the respect for the law.²⁵⁵⁰ Therefore, in addition to the decision to allow international uniform law to emerge by way of organized uniformity through the joint drafting of an intervention, there is also the important question of to whom interpretive and enforcement authority for such an intervention could be entrusted.

An explicit obligation for uniform interpretation is regularly not stipulated in the legal acts of such nature. A number of multilateral conventions contain a general interpretation clause that refers to the importance of uniform interpretation. An example of this is Art. 7 CISG. There, the importance of uniform interpretation for the intended unification of law is regularly emphasized and the wish expressed that the States should strive for its uniformity to the best of their knowledge and belief. In principle, the competence to interpret international uniform law lies with the Parties to the intervention. It is true that these Parties would have the obligation, by signing the regulatory intervention, not to endanger the objectives of the intervention by actions contrary to them. However, we see an obligation to uniform interpretation in the sense that the creation of differences of interpretation constitutes a violation of international law and would rather direct interpretative competence to an international court.

There are essentially two options for enforcement authority. One would be an improvement of international arbitration, the other an “International Court of Justice for Cyberspace Affairs” with regional branches.

International arbitration procedures are familiar with the problem of bringing together different approaches from different legal frameworks. However, in international arbitration, arbitrators are usually appointed by the Parties to resolve a specific dispute. This can be done both after and before the dispute arises. The rules of procedure, the subject matter of the dispute and the applicable law are also determined by the Parties to the dispute, although national law or equity considerations may also be used as a basis for decision. Such a procedure is characterized by a high degree of flexibility. However, we think this flexibility should not be the focus of the intervention, as the main objective of this thesis – as its title already indicates – is an improvement of legal certainty.

Despite a multitude of international legal instruments for the protection of human rights, there are still widespread violations of the right to data protection in the world, which are caused in particular by the insufficient state of legal harmonization of the laws concerned with TFPD. In addition, several human rights courts established to deal with such violations might not have the same level of development as the ECtHR. For proceedings before the existing ICJ, only States can be considered as Parties to the dispute, which we think could endanger the success of the intervention. The “Inter-American Court of Human Rights” (IAGMR) does not have professional judges, nor have all States in Latin and North America or the Caribbean recognized its jurisdiction. The “African Commission on Human and Peoples’ Rights” (ACHPR) was established only after the transformation into the African Union (AU) in June 2002. Asia is still waiting for the establishment of a region-based human rights court. We believe that with the right to data protection, a dynamic and topical issue in the framework of human rights protection could serve as a blueprint for a later even broader protection of other goods within the catalog of human rights by forming an “International Court of Justice for Cyberspace Affairs” with regional branches. However, this should not result in a hierarchical superiority of this court over other international courts and arbitration tribunals. The jurisdiction of this court would

²⁵⁵⁰ Kuner, C. [Christopher]. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 2). *International Journal of Law and Information Technology*, 18(3), 227–247. P. 235.

initially relate exclusively to issues of the regulatory intervention proposed in this thesis; however, later jurisdiction could be extended to all human rights treaties concluded within the framework of the UN. Jurisdiction would accrue to this court through an arbitration clause within the intervention. This could prevent the need for an international treaty between Parties to a dispute, the subject of which would be the appeal to the ICJ for dispute settlement, or an arbitration settlement agreed upon for a specific case. Another central provision in the intervention could be a right of individual redress alike Art. 34 ECHR. The dispute procedure before this International Court of Justice for Cyberspace Affairs could be based on that before the ICJ. Judgments of this court could be final and binding, thus eliminating a crucial weakness of the current system of the UN – the decisions of its organs are not binding on the Parties. This new court, like the ICJ, could be staffed by judges, each of different nationality, representing the main legal frameworks of the world. They could be elected by the UN General Assembly and the UN Security Council by a simple majority vote and be eligible for re-election. Judges could be subject to the incompatibility of their office with other activities and to disqualification in case of bias. A kind of trust fund could also be established under the administration of this court to provide financial support to victims of such violations and their families.

V. Conclusive remarks

To operationalize the preferred option, the intervention should not be a “jack of all trades, master of none”. It should not seek to invent an entirely new approach, scattering both legislative and non-legislative elements in an untargeted manner.

We have made clear that many elements of Convention 108+ could be integrated. We also noted that the orientation of an intervention could be an intentional, binding, organized, with direct effect, self-executing, and unifying treaty based on a monistic approach. The intervention could be initiated by the UN. This organization could not only focus on the lengthy elaboration and consensus-building of the ruleset for the intervention as such, but provide for multi-stakeholder consultation, public education, awareness campaign, sufficient administrative capacity, and resources for UN bodies as part of a holistic strategy, in line with the Commission’s approach to better regulation.

The intervention is a difficult task to accomplish due to its admitted maximum aspiration towards universalism. This observation is based in particular on the fact that the intervention should include essential guarantees and data protection principles of the GDPR, a substitute for the definition of “democratic society”, as well as direct redress of individuals of both judicial and non-judicial nature, and that it would not be sufficient to empower a UN committee or the Council of Ministers.

The introduction of the intervention could, however, be facilitated in a “controlled environment”, apart from the use of a multi-stakeholder approach. This environment could include the means of a sunset clause, adequacy light, and a regulatory sandbox / RPS.

With regard to the transfer mechanism, however, more detailed considerations than in Convention 108+ would have to be made. We believe that a clearer distinction should be made between in-scope transfers and transfers with external relationship. For transfers to in-scope countries, a general free flow of personal data, an ex-post accountability approach and the principle of prohibition of data localization could be standardized. Derogations from this could only be possible for the rationales of “national security / public interest / sovereignty” (including law enforcement) and “universal bads”,

but no derogation for sensitive personal data. For data flows for law enforcement purposes, the intervention could include a commitment to improve existing EIOs and MLATs and model language for new MLATs. In Chapter X, Section II.2 we found an ex-post accountability approach to be “too light” for out-scope transfers. For in-scope transfers, however, this approach has some merits. It could allow a relatively free environment for Parties to the intervention for TFPD, thus meeting parts of the general objective. It could then also fit within the WEF system (DFFT). Moreover, the accountability-based approach is shared by most nations – this includes the US in particular – and could arguably achieve broad consensus on this goal of free data flows alone. The “legal nexus” would not present a difficulty for in-scope transfers, as the intervention would establish uniform substantive law and thus eliminate risks to all stakeholders from differing levels of data protection. Also, an accountability approach for in-scope transfers only would not lead to the application of a national law to a transborder data flow that could potentially encompass all countries in the world, but only the Parties to the intervention. In the case of transfers with an external relationship, the accountability approach could be abandoned and the more restrictive “flow conditional on safeguards” approach selected. A deviation from the principle of free flow of personal data could then be permitted also for sensitive personal data, and for these scenarios the prohibition principle could be standardized for all three rationales. This could ensure that companies that fall within the scope cannot circumvent compliance by transferring personal data to States outside the scope.

Non-legislative elements are numerous and can be divided into policy interoperability, technical interoperability, network interoperability, and regulatory interoperability. Because of the abundance of possible measures in this area, this thesis does not claim to be exhaustive and is devoted only to the most important elements. These could be used to react flexibly to the degree of difficulty of reaching consensus on the legislative elements. As we have already established under the specific objective “cooperation”, legislative elements could be equally complemented with non-legislative elements and – in exceptions – even replaced. There is a need for traditional and non-traditional legal approaches to coordinate or shape the other governance mechanisms; similar conclusions, with which we agree, were drawn by Weber / Staiger:

A mix of old and new rules, as well as their adjustment to new technologies and services, will be the most likely development over the next couple of years. Based on the EU and its strong data protection framework, other countries will seek to mirror these provisions to some extent in order to be able to also process data from the EU. [...] In addition to formal legal rules, an international body should be created with the goal of harmonizing data protection around the globe and provide a forum for discussions and development. This is central to democratic legitimization of any international agreement that may be reached later. [...] Achieving a balanced approach between various challenging problems and the trade-offs that are necessary must be openly discussed in society, taking into account the effects on innovative high-tech environments.²⁵⁵¹

The UN HRC could be the consultative body for the intervention. The interpretative and enforcement authority could be given to a new “International Court of Justice for Cyberspace Affairs” with regional branches, instead of improving international arbitration procedures.

²⁵⁵¹ Weber, R. [Rolf] and Staiger, D. [Dominic]. (2017). *Transatlantic Data Protection in Practice*. Springer. P. 136. // Similarly also already quoted above from Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 341–342.

CONCLUSIONS

Here we list the main conclusions reached in the thesis. The details and justification of each conclusion is to be found in the corresponding section of the thesis.

First

In answering the introductory question about the relevance of “transborder flows of personal data” (TFPD), and the scope of influences that affect such flows, we noted that global capabilities of communication over interlinked networks, over which large amounts of personal data can be exchanged in a timely manner at a low cost, have freed data processing activities – including personal data – from its spatial limitations. The progress of computer technology allows a virtually unlimited number of such activities regardless of time, distance, source, form, and purpose. In addition, the technical knowledge of how to perform these activities at each step of such processing can nowadays be provided as a service by computer manufacturers, software houses, database operators, network operators or service facilities.

Second

There has been a dramatic increase in TFPD which has brought all participants in today’s digitalization from a world of scarce information, typically separated by social spheres and economic areas, into a world of excessive amounts (“Big Data”), availability, flexibility, and scalability of data (“Cloud Computing”), and capabilities of artificial intelligence systems (e.g., “OpenAI’s ChatGPT”) to exploit personal data for social scoring analytics. Innovative forms of technology influence scenarios using personal data in private and public sectors and affect individuals whose personal data are concerned (“data subjects”).

Third

Data location has become less and less important for processing activities including TFPD, as have national borders. The territorial context of TFPD is often unclear, which makes it difficult to trace whether a TFPD has taken place or whether personal data were processed by domestic servers only. Current technology makes the physical location of data practically irrelevant,²⁵⁵² the nationality of the data subject and the country of origin of personal they follow this irrelevance. The connection between ubiquity and virtuality of activities processing personal data has led to an almost unlimited number of governmental and non-governmental databases and of those being responsible (“controllers” / “(sub)processors”) for TFPD.

²⁵⁵² Polcak, R. [Radim] and Svantesson, D. J. B. [Dan Jerker B.]. (2017). *Information Sovereignty. Data Privacy, Sovereign Powers and the Rule of Law*. Edward Elgar. P. 5.

Fourth

Aligned with the approach of Gasser²⁵⁵³, looking at TFPD from cross-jurisdictional perspectives, we identified several “forces at play” within the field of TFPD to make the global dynamism of the topic more understandable. We showed the complex interplay among “dimensions” closely related to another. Such “forces”, which then lead to “changes” in this field of law, were divided into four different “dimensions”: 1) Technology, 2) Economics, 3) Sociology, and 4) Politics.

Fifth

The above-mentioned forces threaten the data subject’s space, as the question of how progress in terms of technology and economics, on the one hand, and the protection of fundamental rights, on the other, might be accommodated with one another, has tilted in favor of what is technically feasible to the detriment of the protection of personal data. This tilt has been underlined by the Snowden revelations in 2013.

Sixth

Legislators started noticing aforementioned forces in the 1960s and regulatory challenges identifying if and how their legal concepts – sometimes norms based on century-old principles and notions – are still applicable to the digital age became apparent. Since 1973, nations around the world have enacted data protection laws at an average rate of three new national laws per year. There are to date around 200 national data protection laws in place. Yet, the legislative pace can hardly cope with the velocity at which technology evolves. A traditional national regulation alone can no longer guarantee an adequate level of the protection of the fundamental right to data protection in TFPD scenarios.

Seventh

States still undertake, according to the positive and negative dimensions of their duties, different measures in trying to balance national interests (especially those of national security / public order / sovereignty) with a free flow of personal data and safeguards for the rights of data subjects. Many nations have already comprehensive data protection legislation in place, others have such in some sectors, while others have no data protection regulations at all. The laws analyzed are explicitly or implicitly, legally binding, or non-binding, by unilateral, bilateral, or multilateral means, geographically based or organizational based. However, only a few of them achieve a comprehensive and mature state, as they generally do not keep pace with technology and lack essential elements. Current data protection laws at the national, supranational, and international level result therefore in a worldwide regulatory fragmentation, which we call a “mosaic”, segregated in different legal “frameworks”.

Eight

The European framework is fundamental rights oriented. It includes a prohibition principle and does not allow a TFPD to third countries or international organizations unless certain conditions are met. It is of binding nature and has extraterritorial reach. Its transfer mechanism has a general scope of application, is conditional on safeguards (“prescriptive”), and has no specific type of data flow restriction. The maturity level of the

²⁵⁵³ Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448. P. 355–374.

European framework is advanced and comprehensive. The essential guarantees are harmonized between GDPR, Convention 108+, the Charter and its interpretations by the CJEU, the ECHR and its interpretations by the ECtHR, and the GDPR and its interpretations by EDPS/EDPB recommendations. This framework sets all eight data subject rights which are known worldwide. All frameworks analyzed in this thesis include the right to be informed, the right to access and the right to correct; other data subject rights show different levels of implementation in the other frameworks. The European framework includes four essential guarantees: (1) Processing should be based on clear, precise, and accessible rules, (2) necessity and proportionality regarding the legitimate objectives pursued need to be demonstrated, (3) an independent oversight mechanism should exist, (4) effective remedies need to be available to the individual. Notwithstanding this fundamentally European pioneering role, it must be noted that European data protection law is not free of flaws either in terms of clarity and legal certainty. Since the development of the GDPR has stagnated and the complexity of the European Framework has increased due to the overlaps of various instruments, especially since the Commission's Digital Strategy, research attention, and thus ours as well, has more and more changed focus to approaches in frameworks from the US and China in particular.

Ninth

The US framework has been internally grappling with an undoubtedly serious conflict of interest in privacy law for a decade. Historically, since the end of World War II, the focus of the US has been on the rationale of national security / public order / sovereignty. For the past decade, however, a rethinking has been taking place, which per se cannot be a quick and easy paradigm shift. This is particularly evident since *Schrems II* and the reactions to it in the US. The US framework shows significant differences in the levels of development when comparing US federal and US State level. Some US states, such as California in particular, have reached a level like the European framework. The federal level, however, is a "piecemeal" / "patchwork", though ADPPA represents a promising federal law currently in the legislative process. The US framework is trade oriented. It has no prohibition principle, though ADPPA would include this for certain types of sensitive personal data. Its data protection framework is binding. Extraterritorial reach has at federal level only the Cloud Act; and some State laws, such as California, Colorado, Connecticut, and Virginia. Its transfer mechanism has a sector-specific scope of application and an ex-post accountability approach ("light touch" approach), with some local storage requirements. Its maturity level is progressing with ADPPA leaving aside; with ADPPA it would be advanced. The US framework is sector-oriented and not comprehensive. ADPPA would include the same seven principles as the GDPR at federal level and six data subject rights known to the GDPR, though the right to restrict the processing of personal data and the right in relation to automated decision making and profiling only partially. At US State law level, California, Colorado, Connecticut, and Virginia are like the data subject rights guaranteed by the GDPR, though a private right of action exists only in California (and in a limited way). As to the essential guarantees set above by the GDPR as a "gold standard", the fulfillment of guarantees regarding independent oversight and effective remedies is insufficient in the US framework.

Tenth

Within the APAC framework, a distinction must be made between APEC, ASEAN, and China for certain parts. Leaving China aside, the APAC framework is trade-oriented, has no prohibition principle, is only binding for Parties to the CBPR and has no extraterritorial effect. Its maturity level is progressing and of self-regulatory nature. Compared to the

European data protection principles, APEC lacks the storage limitation principle and ASEAN the data minimization principle. Both APEC and ASEAN do not guarantee minimum two data subject rights which are included in the European framework. APEC lacks the essential guarantee of effective remedies, while ASEAN lacks both that and that of independent oversight.

Eleventh

After an analysis of China's rule-setting, which for a European lawyer is proceeding at an astonishing speed, we found that the Chinese system is – from the perspective of an apt rule-setting process in a mature framework – very well elaborated. It almost seems as if the Chinese legislator has taken the best borrowings from the GDPR and adapted them to national interests. China protects those, e.g., by requiring OCII to store “important data” in China. China shows a mixture between security-, trade-, and fundamental rights oriented. It introduced GDPR-like restrictions, though on specific types and sectors. Its laws are binding and have extraterritorial effect. China's transfer mechanism is sector-specific and data type specific, ad-hoc authorization (high level of restrictiveness), local storage, local processing and local access is required. We consider China's national laws as reaching an advanced and comprehensive level of maturity. PIPL includes the same data protection principles and data subject rights as the European framework. As to the essential guarantees compared with the other frameworks, China's CAC might not have sufficient independence, and Art. 38(4) PIPL is not precise and transparent enough, as the clause “where it has satisfied other conditions prescribed by laws, administrative regulations, or the State cyberspace administration” opens the State too many possibilities for interpretations.

Twelfth

As for the International organizations legal framework, OECD and WTO are trade oriented, the UN puts a stronger focus on fundamental rights. Both OECD and UN have no prohibition principle in place, the WTO is silent on a default position. This framework is of nonbinding nature and has no extraterritorial effect. Its maturity level is progressing and self-regulatory. The UN lacks the data minimization, storage limitation and accountability principle. The OECD lacks storage limitation and data minimization principles. All International organizations do not guarantee minimum two data subject rights which are included in the European framework. Similar applies to the essential guarantees: OECD and UN lack aforementioned guarantees on independent oversight and effective remedies.

Thirteenth

Self-regulatory measures are important whenever the general objective of this thesis can only be resolved with the support of the specific objectives of “collaboration” and “trust”. Under the blended governance approach this thesis puts forward, the harmonizing intervention should also include measures that involve non-legislative elements. Establishing collaboration is more relevant for out-of-scope scenarios than for in-scope scenarios, as in the latter, a consistent level of protection is ensured by transfer mechanism, principles, essential safeguards, and maturity, which are consistent on a consensus basis and integrated into the intervention. However, integrating the idea of “data flow where there is trust”, for the intervention to be successful more than uniform rules is required, even for in-scope scenarios.

Fourteenth

By presenting the normative frameworks in Chapters II–VII, we have provided the answer to our first research question: “Which are the rules in legal frameworks at global level that affect TFPD?” Despite the developments in the US and APAC (dominated by the rule-setting in China) frameworks, the observation remains that data protection, understood as a procedural limitation of the “freedom” of processing personal data to protect the privacy of the individual, is still a phenomenon shaped by European influences, especially those of the GDPR of 2016. The European framework is the most developed framework as of today. Significant improvements of Convention 108 (which is also based on European influences, but in this case on the Council of Europe) have been accomplished by Convention 108+. GDPR and Convention 108+ encompass the same data protection principles and essential guarantees, which both represent the largest extent worldwide.

Fifteenth

The current regulatory mosaic is complex and unclear in many parts, the TFPD cosmos highly multi-layered and difficult to oversee. We consider the current regulatory system as “deficient” in comparison to the best *possible* legal system that does not yet exist. This new legal system would need to be designed in such a way that it could safely achieve the desired objectives of the international community for the information society, namely its development-oriented, human rights-sensitive design based on the UN Charter, international law and the UDHR. Normative deficits exist in regulation and implementation if the normative order of the Internet, consisting of international law rules, European law, State law, private legal regimes and soft law, does not legitimately and effectively achieve these objectives. These deficits indeed exist. To approach that deficiency, we considered the concept of “Smart Regulation” and finally used the concept of “Better Regulation” – the latter being a central point of reference for the regulatory policy in the OECD and the EU. We chose to follow the structure of a Regulatory Impact Assessment (“RIA”) from EU law. The reason for this is that a RIA improves the quality of new legislation and ensures a continuous and coherent review of law to achieve the objectives of legislative action as effectively and efficiently as possible.

Sixteenth

Aforementioned deficiency raises a number of “problem drivers”. These resemble in sum the basic driver for relevance of the legal issue, which is why our description of the dimensions was important. The Commission described in one of its “problem trees” of the Better Regulation approach the “expansion of scale and scope of data processing as a facilitator of new technologies & innovation”²⁵⁵⁴ as basic driver, which then affects a “core problem”. We therefore categorized problem drivers to a “core problem” and other two problem categories, the “different approaches to the nature and scope of the right to data protection” and “extraterritoriality and blocking statutes”. We addressed these in Chapter VIII in response to our second research question: “Which problem categories and problem drivers arise from the lack of harmonization in this field of law?” These problems bring legal uncertainty and contrast with the fact that the global development of data protection law is proceeding in an interdependent process in which the aforementioned four dimensions of technology, economics, sociology, and politics interact with each other. The problem drivers and problem categories identified

²⁵⁵⁴ European Commission. *Commission Staff Working Document. Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, SWD(2017) 304 final*, (13 September 2017). P. 4.

complicate the lawful behavior of multinational enterprises (“MNEs”) and can have negative consequences for the progress of the globally operating digital economy. Many jurisdictions are *per se* in flux in this legal matter and are constantly adapting to new circumstances. Changing conceptions of social morality create, among other things, incrementally increasing pressure for change. The formation of social will, which is also addressed in the sociological dimension, and the legal system are therefore in mutual communication with each other, but with a delay factor compared to the technological dimension.²⁵⁵⁵ The current situation led global tech standard-setting becoming a new battleground for techno-nationalism, thus more protectionism, which threatens our proposed intervention’s general objective of harmonization. This brings us to the core problem identified of in this thesis, which is the dilemma of a free flow of data vs. data flow restrictions. The goal of a free flow of personal data is manifested in all relevant regulatory instruments discussed in this thesis. At the same time, however, regulatory measures to restrict such flows increased. Such measures reduce competition, increase regulatory complexity, harm innovation, and stifle economic growth. They are ultimately a paradox, because calls for greater sovereignty at a time when disruptive technologies require greater international focus are hindering cooperation to solve emerging problems.²⁵⁵⁶

Seventeenth

As to the type of the process which should be followed to achieve such the regulatory intervention sought, we found that the commitment to one solely comparative law method would have been unrealistic. If our approach is at all close to a particular comparative law method, that is the “functional method”. In this regard, we note that the instrument should be drafted by legal experts in a “multi stakeholder approach”, and then be incorporated into an international treaty.

Eighteenth

The state of research to date has been particularly thin in describing the interests of all stakeholders in a global ecosystem of TFPD and in grouping the different laws to specific legal framework archetypes regarding the regulation of TFPD. We considered the endogenous and exogenous variables in the global ecosystem of TFPD resulting in different framework archetypes. In doing so, we answered our third research question: “Within a global ecosystem of TFPD, can regulations be categorized under some framework archetypes, what are the differences between those, and do those have common principles and essential guarantees regarding TFPD?” We identified which set of different interests prevail in the global ecosystem of TFPD and could oppose the intention of a regulating organization. Bringing the totality of these interests into harmony as far as possible, especially assigned to regulatory “arenas” (such as the most important one, the EU-US arena) and thereby arriving at a possible consensus for rule-setting, has so far also not been sufficiently considered in the literature. We have mapped these interests to different and non-mutually exclusive “elements” of an architecture for global governance, like the WEF²⁵⁵⁷, and found that these elements can be divided into “universal availability and “limited participation.”

²⁵⁵⁵ “It is a truism that the law lags behind technology”. See Buttarelli, G. [Giovanni]. (2020). Foreword. In C. [Christopher] Kuner and L. A. [Lee A.] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. v–vi). Oxford University Press. P. v.

²⁵⁵⁶ Hörnle, J. [Julia]. (2021). *Internet jurisdiction*. Oxford University Press. P. 437.

²⁵⁵⁷ WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*.

http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf. P. 14.

Nineteenth

We made the policy choice of setting the general objective, of pursuing an intervention that, in the interest of effective protection of fundamental rights, harmonizes the existing data protection regulations and reduces currently raising restrictions to a free flow of personal data, which should safeguard a TFPD and enable the digital economy to operate efficiently and to deliver benefits more rapidly in multiple nations and regions.

Twentieth

To achieve the general objective, we set several specific objectives, namely, consensus, universality, human-centricity, maturity, trust, cooperation, and innovation. We disagree with the argumentation that supranational or even national regulations in a certain region are preferable to those of a universal approach. Innovative technological progress and the protection of fundamental right can be accommodated with one another. We believe that protecting and sharing personal data are not mutually exclusive. A strong data protection system facilitates the exchange of data, as it enables consumers to trust those participants in the global digital economy that care about the careful handling of their customers' personal data. High data protection standards thus represent an advantage in the economy having strong data protection mechanisms in place. The same applies to cooperation in relation to law enforcement: essential data protection guarantees are an integral part of the effective and rapid exchange of information in the fight against crime, based on mutual trust and legal certainty. We think that an intervention needs a global trust structure, because, to enable trustworthy transfers, a basis is required that minimizes risks and creates equal opportunities between the stakeholders. In this respect, we agree with the WEF's approach²⁵⁵⁸ to the greatest possible extent. An intervention should be – in the totality of its subject matter – as consistent as possible with most of the frameworks, as this would facilitate consensus. However, this subject matter includes not only transfer mechanisms, principles, and essential guarantees, but everything that determines the stage at which all data protection measures should be in place. A specific objective should therefore also be to regulate an as high as possible level of maturity in the intervention according to both the GSMA classification and the de Terwangne classification,²⁵⁵⁹ and to find consensus for this level. We have chosen to follow a human-centric, thus a fundamental-rights based, and not a trade-oriented approach to the problems. We note that Weber / Staiger²⁵⁶⁰ prefer a “hybrid” approach, which we follow in parts because of the necessary non-legislative elements, but their approach seems too non-binding to us.

Twenty-first

A combination within the aforementioned objectives does not necessarily constitute a “conflict of objectives”. We think it is necessary to use a balancing tool, to give greater weight to the protection of personal data on the Internet, and to minimize problems in the process. However, balancing stakeholder interests should not be done for its own sake; rather it must retain that, as Art. 1 of the Charter, states: “Human dignity is inviolable. It must be respected and protected.” Potential conflicts should be resolved by weighing of interests. An international legal instrument should only be sought at all if the objectives of such an intervention cannot be sufficiently realized by the nation States (“efficiency test”) but can be better realized at the international level because of their scope and

²⁵⁵⁸ WEF. (May 2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf.

²⁵⁵⁹ See Chapter IX, Section III.1.5.

²⁵⁶⁰ Weber, R. [Rolf] and Staiger, D. [Dominic]. (2017). *Transatlantic Data Protection in Practice*. Springer.

effect (“added value test”). To fulfill proportionality, a weighing of interests focuses primarily on an economic assessment. It should therefore also not be possible to fulfill the same policy objective in a way that has a less restrictive effect on trade; this position was also taken by the OECD.²⁵⁶¹ We found that the intervention we propose would bring an added value to an inefficient nation States’ solution and would comply with proportionality.

Twenty-second

We found that the best option for the intervention sought is a sophisticated combination of legal rules at the international law level. These rules should aim at harmonizing existing rights and making them as uniform as possible. These rules do not require a fundamental reorganization of international law, but rather a defined content and rule-setting process. Legislative approaches may be distinguished based on their “direction” (either “bottom-up” or “top-down”), and on the “intensity” of the harmonization sought. We found that national / supranational laws must be supplemented by a public international law perspective, especially when it comes to a necessary transfer of sovereignty from the national / supranational level to the international level, which is what is needed, at least in part, for harmonization at the international level. This makes our approach overall top-down, nevertheless with a strong recognition of bottom-up elements. In terms of intensity, we opt for a binding effect of the intervention whilst striving for the optimum of uniformity. We found that the necessary approach to regulate aforementioned forces at play – technology, economics, sociology, and politics – was for us the “blended governance” rather than a strictly law-based approach. This led us to examining four different avenues of response: technological approaches such as Privacy Enhancing Technologies; the possible role of market forces and other market-based mechanisms; a human-centric response to the fundamental right to data protection affected; and traditional and non-traditional legal approaches to coordinate or shape the other governance mechanisms. We found that the basis for the envisioned intervention should be the “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (Convention 108) in its modernized version (Convention 108+), and that the bodies to promote and enforce those new rules should be the “United Nations Human Rights Council” (UN HRC) and a new International Court of Justice for Cyberspace Affairs with regional branches.

Conclusions nineteenth to twenty-second answer our fourth research question: “What objectives and options could a regulatory intervention have?”.

Twenty-third

We have shown in Chapter XII that, to be able to provide for a global consensus on an adequate level of data protection while enabling efficient TFPD, however, two tools known in political science and transferable to the legal questions of this thesis must be used: Upward Convergence and Downward Convergence. While we have found that Convention 108+ provides the most feasible basis for a ruleset, there is a need for adaptation to reach consensus for regulatory intervention by the UN. For the sake of consensus, the expression “in a democratic society” used in various national, supranational, and international regulations, should be omitted. We believe that at the level of a human-centric, i.e., fundamental rights-based data protection law, cooperative

²⁵⁶¹ Organization for Economic Co-operation and Development. (21 December 2018). *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, [https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP\(2018\)19/FINAL&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/FINAL&docLanguage=En). Para. 17.

relationships should also be entered into with countries such as China, which, admittedly, still leave themselves too vague clauses in their national data protection laws for the defense of national interests. We also found that the intervention should be an intentional, binding, organized, with direct effect, self-executing, and unifying treaty based on a monistic approach. We noted that specific objectives “oscillate” between hard law and soft law components. Both sides are indispensable for the intervention and follow the blended governance approach. Of importance for a distinction between hard law and soft law components is whether a TFPD scenario takes place between States being Parties to the intervention (in-scope States), between in-scope States and out-of-scope States (being non-Parties), or between out-of-scope States. Within the intervention, the rules would be harmonized, mature and human-centric; in this regard, mainly hard law components such as a general free flow of personal data, an ex-post accountability approach, and the principle of prohibiting data localization measures should be applied. The more a TFPD turns to a scenario with external relationships, the more the solution should consist of soft law components. The latter applies in particular to the specific objectives of trust, innovation, and cooperation; and within the latter to interoperability. As a transfer mechanism, the “conditional on safeguards” approach accessible to companies of all sizes and not only sector-specific should be used, as this allows the greatest possible flexibility. However, several derogations are necessary to allow countries such as China under certain conditions to protect legitimate interests. The general scope of transfer mechanism should allow data flow restrictions for certain data types under conditions based on the rationale of national security / public order / sovereignty, including law enforcement, but none for sensitive personal data. However, such a legitimate public policy objective would then have to submit to the necessity test under Art. XIV GATS. The intervention should include all principles and essential guarantees of the European framework. In fact, a main advantage from China is a well thought-out and consistent system on a level almost as high as that of the European framework. Data flows for law enforcement purposes could be covered by a commitment to improve existing European Investigation Orders (“EIOs”) and Mutual Legal Assistance Treaties (“MLATs”) and model language for new MLATs.

Twenty-fourth

Although a solution on an international level such as the UN could take much time and could be vetoed by one of its Security Council Members, we submit that the intervention should be initiated by the UN. This should be done in a controlled environment, namely a regulatory sandbox. The UN Human Rights Convention should be the consultative body for the intervention, and the interpretative and enforcement authority should be given to a new International Court of Justice for Cyberspace Affairs with regional branches, instead of improving international arbitration procedures. The UN should work multilaterally for greater upward and downward convergence of data protection principles and essential data protection guarantees worldwide. At the same time, the UN should use transfer instruments to safeguard data protection rights and assist economic operators when transferring personal data to countries whose laws do not ensure an adequate level of data protection according to the regulatory intervention. These tools should also be used to further facilitate cooperation between the UN’s supervisory and law enforcement agencies and their international partners. The UN should promote harmonization of high levels of data protection internationally to enhance law enforcement cooperation, contribute to free trade, and develop human-centric protection in the area of TFPD.

With conclusions twenty-third and twenty-fourth we answered to our fifth and last research question of this thesis: “What regulatory content could such intervention have

to find a reasonable compromise among the most important stakeholders affected, to act in favor of a worldwide convergence of regulations on TFPD, and how could the process of law-making and enforcement be?”

EPILOG

As mentioned at the outset, the research conducted for this thesis finished on 30 June 2023, and therefore any new developments after that date could not be included. Consequently, the thesis does not deal with the EU Commission's implementing decision made on 10 July 2023,²⁵⁶² when the thesis was already final and closed, and only a few days away from the submission deadline.

Admittedly, this Commission's decision, which determines an essentially adequate level of protection of personal data under the EU-US DPF caused us some headaches. While, as noted, it is beyond the temporal scope of this research and thus not included in the thesis, we cannot leave the developments in July 2023 in the EU-US arena completely unmentioned. Therefore, if briefly, we will consider them in this EPILOG – and will certainly elaborate on them regarding the potential publication of this thesis as a monograph.

On 3 July 2023, the US Department of Justice and the Office of the US National Intelligence Director announced the completion of commitments under POTUS Joe Biden's "Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities" (EO 14086)²⁵⁶³ concerning the EU-US DPF:

Today, the United States has fulfilled its commitments for implementing the EU-U.S. Data Privacy Framework (EU-U.S. DPF) announced by President Joe Biden and European Commission President Ursula von der Leyen in March 2022. This represents the culmination of months of significant collaboration between the United States and the EU and reflects our shared commitment to facilitating data flows between our respective jurisdictions while protecting individual rights and personal data.²⁵⁶⁴

On the same day, the US Office of the Director of National Intelligence (ODNI) released policies and procedures the US IC have to follow as part of the EO 14086.²⁵⁶⁵ The week before, US Attorney General Merrick Garland had designated the EU and the EEA as

²⁵⁶² European Commission. (10 July 2023). *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final. // This decision entered into force on 11 July 2023.

²⁵⁶³ United States of America, The White House. *Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>, (7 October 2022).

²⁵⁶⁴ US Department of Commerce. (3 July 2023). *Statement from U.S. Secretary of Commerce Gina Raimondo on the European Union-U.S. Data Privacy Framework*. <https://www.commerce.gov/news/press-releases/2023/07/statement-us-secretary-commerce-gina-raimondo-european-union-us-data>.

²⁵⁶⁵ US Office of the Director of National Intelligence. *ODNI Releases Intelligence Community Procedures Implementing New Safeguards in Executive Order 14086*. <https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086>.

“qualifying states”²⁵⁶⁶ under EO 14086 and the Biden administration announced that it had implemented all the steps agreed with the Europeans in US law.²⁵⁶⁷ These actions

were linked because the final adequacy decision [of the Commission] could only be issued once the EU and its member states had received the designation as “qualifying states”. [...] Under Executive Order 14086, a country can be designated as “qualifying” if it meets three requirements. First, the country must provide “appropriate safeguards in the conduct of signals intelligence activities for United States persons’ personal information that is transferred from the United States” to the qualifying country or region, such as the EU. Second, the qualifying country or region must permit the transfer of personal information for commercial purposes. Third, the designation must “advance the national interests of the United States.”²⁵⁶⁸

This addressed the above-mentioned problem of reciprocity for international cooperation, especially for law enforcement purposes.²⁵⁶⁹ Alex Greenstein, Director of the EU-US DPF at the US Department of Commerce and head of the Privacy Shield for 4 years, commented on the long process of getting this EU-US DPF finalized in an event hosted by the IAPP on 14 July 2023:

What we put in place here was narrowly targeted at addressing the two buckets of issues that the Court [CJEU] was concerned with. One was on the necessity and proportionality of US surveillance practices. That was addressed in the Executive Order [EO 14086]. The other issue was redress, the ability of European persons to complain and have their case heard if they think that they have been inappropriately have their data accessed. The Executive Order [EO 14086] and the accompanying Attorney General’s regulation set up a new redress mechanism, a Data Privacy Review Court, which expands a binding and independent redress mechanism. The third component is the Data Privacy Framework Program, which is the actual transfer mechanism that companies can sign up for and use to transfer data from Europe to the US. [...] That was really our goal, in conjunction with the commission, was to really craft something that directly addressed the concerns raised by the court and so I think we did a pretty good job of that. [...] We had to work under certain constraints in terms of what we could do within the U.S. law and Constitutional framework, but I think that also let us be very creative, and work very closely with the Commission to understand what the obligations were that the court put out there and also how to use what we have available in the United States to meet those.²⁵⁷⁰

These actions on the US side paved the way for the Commission to now recognize that the level of protection for personal data in the US is essentially equivalent. The Commission concluded on 10 July 2023 that it

²⁵⁶⁶ United States of America, Department of Justice, Office of the Attorney General. *Designation Pursuant to Section 3(f) of Executive Order 14086, 205-30*, <https://www.justice.gov/d9/2023-07/Attorney%20General%20Designation%20Pursuant%20to%20Section%203%28f%29%20of%20Executive%20Order%2014086%20of%20the%20EU%20EEA.pdf>, (30 June 2023). // The US Department of Justice had published a detailed, 34-page memorandum explaining the legal rationale for the attorney general designation, see United States of America, US Department of Justice. *Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086*, <https://www.justice.gov/d9/2023-07/Supporting%20Memorandum%20for%20the%20Attorney%20General%27s%20designation%20of%20EU-EEA.pdf>, (20 June 2023).

²⁵⁶⁷ See Chapter IX, Section III.3.

²⁵⁶⁸ Swire, P. [Peter]. (18 July 2023). *A guide to the attorney general’s finding of ‘reciprocal’ privacy protections in EU*. <https://iapp.org/news/a/a-guide-to-the-attorney-generals-finding-of-reciprocal-privacy-protections-in-eu/>.

²⁵⁶⁹ Chapter VIII, Section III.; and Chapter XII, Section III.1.

²⁵⁷⁰ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

considers that the United States – through the Principles issued by the U.S. DoC [US Department of Commerce] – ensures a level of protection for personal data transferred from the Union to certified organizations in the United States under the EU-U.S. Data Privacy Framework that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679. Moreover, the Commission considers that the effective application of the Principles is guaranteed by transparency obligations and the administration of the DPF by the DoC. In addition, taken as a whole, the oversight mechanisms and redress avenues in U.S. law enable infringements of the data protection rules to be identified and punished in practice and offer legal remedies to the data subject to obtain access to personal data relating to him/her and, eventually, the rectification or erasure of such data. Finally, on the basis of the available information about the U.S. legal order, including the information contained in Annexes VI and VII, the Commission considers that any interference in the public interest, in particular for criminal law enforcement and national security purposes, by U.S. public authorities with the fundamental rights of the individuals whose personal data are transferred from the Union to the United States under the EU-U.S. Data Privacy Framework, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists. Therefore, in the light of the above findings, it should be decided that the United States ensures an adequate level of protection within the meaning of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union, for personal data transferred from the European Union to organizations certified under the EU-U.S. Data Privacy Framework. Given that the limitations, safeguards and redress mechanism established by EO 14086 are essential elements of the U.S. legal framework on which the Commission's assessment is based, the adoption of this Decision is notably based on the adoption of updated policies and procedures to implement EO 14086 by all U.S. intelligence agencies and the designation of the Union as a qualifying organization for the purpose of the redress mechanism that have taken place respectively on 3 July 2023 (see recital 126) and 30 June 2023 (see recital 176).²⁵⁷¹

Ultimately, those developments in the US framework, and the Commission's following decision in the European framework do not change the results of this thesis. The EU-US DPF temporarily aims at the realization of the general objective of the thesis²⁵⁷², though only for scenarios of transatlantic TFPD between EU and US. Anonymization is now also included in the EU-US DPF.²⁵⁷³ The US is working on the EU-US DPF providing for the extension to other countries, which would be in line with the principles of openness, trust, and interoperability²⁵⁷⁴; companies from, e.g., the UK would first need to participate in the EU-US DPF before being allowed to extend their commitments to also apply to the UK.²⁵⁷⁵ Similarly, for the end of 2023, the US foresees to bring the inclusion to Switzerland in force, although not as a simple extension of the EU-US DPF but a standalone text. The validity of these extensions then depends on the declaration of adequacy by the UK's and the Swiss SAs. Nevertheless, as noted by Alex Greenstein, Director of Data Privacy Framework at the U.S. Department of Commerce,

²⁵⁷¹ European Commission. (10 July 2023). *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final. Paras. 201–204.

²⁵⁷² See Chapter X, Section I.

²⁵⁷³ "Key coded data is now covered as well. That shouldn't change companies' commitments in that regard because they couldn't use Privacy Shield for transfer, so this is an extension of what you can do with the DPF [the EU-US DPF]". See Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁷⁴ See Chapter X, Section II.5.

²⁵⁷⁵ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

the EU-US DPF is fairly particularized at this point to be generally a protection regulation. I don't think that we presently anticipate expanding it to other countries. We are strongly supporting the CBPR rules internationally as a multilateral approach to data privacy best practices. Right now, we are focused on getting the EU, Switzerland, and the UK done and in place.²⁵⁷⁶

This means that non-European countries with local data export regimes cannot join the EU-US DPF, it is not intended as a multilateral approach. The scope of the EU-US DPF is again "sectoral" because it requires – like the Safe Harbor – an act for US companies to submit to all rights and obligations of the EU-US DPF. Only companies falling under the jurisdiction of the FTC or the Department of Transportation can commit themselves to the EU-US DPF. An expansion of the EU-US DPF to, e.g., non-profit organizations and the finance sector is a long running issue the US is working on, according to Alex Greenstein.²⁵⁷⁷

For a US company to be considered a secure data recipient and to comply with the EU-US DPF, it must go through a self-certification process led by the US Department of Commerce. This requires an organization to submit several documents. If these are complete, the organization is added to the EU-US DPF list²⁵⁷⁸ of participating companies and is considered to be self-certified under the requirements of the EU-US DPF. Companies that were already certified under the Privacy Shield can now update their privacy notices within a three-month transitional period (beginning on 17 July 2023) to the newly added requirements in the EU-US DPF. Once a US organization is certified, it must renew that certification each year (the re-certification date under the Privacy Shield will count for the re-certification date of the EU-US DPF). Companies not wanting to participate in the EU-US DPF will be provided with formal withdrawal process documents, similar to those under the Privacy Shield. Alex Greenstein said also that

it's worth noting that the decision [*Schrems II*] was focused solely on national security issues and government access to that surveillance and really did not say anything about the commercial protections offered by Privacy Shield. [...] We took as our base the Privacy Shield principles and lightly updated them because the *Schrems II* decision group trying to address didn't really raise any questions about commercial protection. So, we didn't really need to change the commercial elements of the Framework [EU-US DPF]. European partners saw the benefit in having a great deal of continuity and that's why we really focused on, for transition from Privacy Shield to Data Privacy Framework, that companies should not have to change their practices and operations. Companies registered under Privacy Shield can smoothly move over to the Data Privacy Framework [EU-US DPF].²⁵⁷⁹

On 17 July 2023 at 16.00h CET – the same day the website including this list²⁵⁸⁰ was launched – 2,602 companies were already registered in this list. This suggests that, as Maximilian Schrems put it,²⁵⁸¹ rather a "copy & paste" in this transition from Privacy Shield to EU-US DPF than a comprehensive self-certification process is currently taking

²⁵⁷⁶ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁷⁷ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁷⁸ This has been set up on 17 July 2023. // International Trade Administration, U.S. Department of Commerce. *Data Privacy Framework (DPF) Overview*. <https://www.dataprivacyframework.gov/s/program-overview>.

²⁵⁷⁹ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁸⁰ International Trade Administration, U.S. Department of Commerce. *Data Privacy Framework (DPF) Overview*. <https://www.dataprivacyframework.gov/s/program-overview>.

²⁵⁸¹ NOYB. (10 July 2023). *New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield". noyb will challenge the decision*. <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.

place. Also of concern is that the Privacy Shield principles have only been “lightly updated”. We observed further that fundamental surveillance issues were not sufficiently addressed in the EU-US DPF. We also doubt the independence of the US Data Protection Review “Court” from the perspective of the standards set by EU law, as this Court still sits within the US executive branch.²⁵⁸² Mr. Greenstein also commented on the procedural steps a company registered under the Privacy Shield should conduct:

They should begin applying those [EU-US DPF] principles, to update the privacy policies [including the correct referencing to the EU-US DPF instead of the Privacy Shield] to reflect the Data Privacy Framework [EU-US DPF], to have these companies moved directly into the Data Privacy Framework [EU-US DPF]. [...] They should be changing references from Privacy Shield to the DPF and also change any related references to the GDPR.²⁵⁸³

He gave the impression it in the conference as if only some references and light adjustments in the privacy policies of the companies self-certified under the Privacy Shield would be necessary for the transition to the EU-US DPF.

Mr. Greenstein commented further that “the national security commitments that we have made in the Executive Order [EO 14086] and the redress mechanism, those apply across all transfers, so should also provide greater assurance for companies using those mechanisms”²⁵⁸⁴. A similar statement was made by European Commission’s Bruno Gencarelli, saying that the US commitments have been designed to apply to “any transatlantic data flow regardless of the instrument to use”. Data protection professionals therefore raised these questions:

- With the commitments under EO14086 applying to all data transfer mechanisms, this means that EU companies transferring data to the US under SDPC can now just do without implementing any supplementary measures?
- Can a TIA simply refer to the essential equivalence provided by the EO 14086 and the new redress court and reflect in the TIA that this equivalence applies to all transfer mechanisms and also refer to the fact that the Commission’s adequacy determination says “for those participating in the EU-US DPF”, pairing the commercial and the national security elements?²⁵⁸⁵

Gencarelli affirmed that “EU organizations using alternative mechanisms like SCCs [SDPC] and BCRs can now show on transfer impact assessments [TIAs] that requirements around national security and government access are fulfilled and compliant under the DPF’s enhanced protections”²⁵⁸⁶. Mr. Greenstein’s answer to the concerns raised regarding the overlap between the different legal bases set by Arts. 45 ff. GDPR was that it “makes sense to reference the adequacy decision in a TIA. The competent SA [for those responsible for the TFPD] should be consulted about what needs to be included in a TIA. Certainly, (companies) need to consult with their SAs about what that

²⁵⁸² “The Data Protection Review Court has sort of a great deal of independence, but still sits within the executive branch.”, See Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁸³ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁸⁴ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁸⁵ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁸⁶ Gencarelli, Bruno. (20 July 2023). *EU data transfers: The latest and what comes next*. <https://www.linkedin.com/events/708678149106577472>.

means in practice”²⁵⁸⁷ The “doubling up” using both SDPC and the DPF remains largely unclear. Mr. Greenstein indicated that “there were concerns around the ability of companies to use other data transfer mechanisms such as the Standard Contractual Clauses [SDPC] and Binding Corporate Rules [instead of the EU-US DPF]”²⁵⁸⁸ and that the principles of the DPF can help to concretize SDPC. Until further guidelines on the Commission’s adequacy decision regarding the EU-US DPF are published in the weeks to come, there are still legal uncertainties in the details. Connecting the EU-US DPF with US federal level has been also addressed by Gencarelli saying that enacting a federal law “that would offer strong safeguards could also, depending on its content, potentially extend the scope of the Data Privacy Framework”.²⁵⁸⁹

We think that, in practice, data protection measures (after having conducted the certification process, which starts after the 3 months transition period and must be conducted within 1 year) of such companies will provide indications for the effectiveness of the EU-US DPF in the future and whether there is really “continuity in coverage”. Overall, we think substantial adjustments in FISA would have been the chance for real changes because no agreement will work without a legal change to the mass surveillance of EU citizens. The Commission missed the chance to bring about this change at US federal level, to the detriment of the EU economy and beyond.

We challenge to what extent the Commission, which is assigned the role as guardian of the EU treaties, was guided in its decision more by political-economic than by fundamental rights considerations. Therefore, despite this “first aid kit” or even only a “plaster” applied in July 2023 (which we expect will be removed by a *Schrems III* case before the CJEU) on the TFPD issues within the EU-US arena, there is – half a century after the first national data protection law in 1973 – still no global sustainable solution in place by one law to rule them all. As expected, NOYB noted already on the day of the Commission’s decision on the EU-US DPF, that this “third attempt of the European Commission to get a stable agreement on EU-U.S. data transfers will likely be back at the Court of Justice (of the European Union) in a matter of months”²⁵⁹⁰. Gencarelli and Greenstein reiterated that they can credibly defend this framework.²⁵⁹¹ Maximilian Schrems went even further by commenting:

They say the definition of insanity is doing the same thing over and over again, yet expecting a different result. Just like Privacy Shield, the latest agreement [the EU-US DPF] is not based on substantive changes, but on short-term political thinking. Once again, the current Commission seems to be passing this mess on to the next Commission. FISA 702 needs to be renewed by the US this year, but with the announcement of the new agreement, the EU has lost any leverage to get FISA 702 reformed. We have now had “Harbors”, “Umbrellas”, “Shields” and “Frameworks” – but no substantive change to US surveillance law. The press statements of today are almost a verbatim copy of those of 23 years ago. Merely claiming something is “new”,

²⁵⁸⁷ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*.

<https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁸⁸ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*.

<https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.

²⁵⁸⁹ Gencarelli, Bruno. (20 July 2023). *EU data transfers: The latest and what comes next*.

<https://www.linkedin.com/events/708678149106577472>.

²⁵⁹⁰ NOYB. (10 July 2023). *New Trans-Atlantic Data Privacy Framework largely a copy of “Privacy Shield”. noyb will challenge the decision*. <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.

²⁵⁹¹ Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*.

<https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>. // Gencarelli, Bruno. (20 July 2023). *EU data transfers: The latest and what comes next*. <https://www.linkedin.com/events/708678149106577472>.

“robust,” or “effective” is not enough before the Court [CJEU]. We needed a change in US surveillance law, and it doesn’t exist.²⁵⁹²

Concerns about an appropriate protection of the fundamental right to data protection during a TFPD scenario had already become known to a broad public and thus to a large amount of data subjects not least through the Snowden revelations a decade ago. Efforts to find a stable solution, especially in the EU-US arena, started almost a quarter of a century ago and have not yet been fruitful. Maximilian Schrems once stated that

we really have to now find a solution that’s stable and works for the long term. It can’t just be a privacy umbrella or a Safe Harbor III that will go down the drain the same way. [...] There is no room for another treaty or something to overcome the problem. Sometimes I say it’s like basically two trains colliding and then you add a third train, but that will be smashed, as well. There’s just no room for an executive agreement when you have these different obligations on a legislative level.²⁵⁹³

A binding international regulatory instrument on TFPD would not be easy to implement, but feasible. Greenleaf quite pointedly but aptly expressed that in relation to both modernization and globalization, an intervention at the international level could achieve to “pass the Goldilock Test: not too hot, not too cold, but just right”²⁵⁹⁴. We believe that from the principles of democracy and human rights protection, international law in the area of TFPD should develop into a kind of world law under strong international organizations with their own jurisdiction. A decade ago, this would have been unthinkable, as fewer countries worldwide had data protection laws in place, exogenous and endogenous interests of the stakeholders involved in a lawmaking process were therefore yet largely unknown, and a (even partial) common understanding did not exist. We have explained how one could come closer to a regulatory instrument that is as universal as possible. An aspired universalism, however, is often apolitical. We cannot accept that strategic thinking is sacrificed for an idealistic world view. Universalism with its theory of progressive juridification of international relations corresponds well to the strategic interests of a “middle power” like the reunited Federal Republic of Germany: too strong to depend on imperial protection, too weak to protect others effectively. This also applies to several other countries around the world, including those of the “global south”. A podcast half a year after the beginning of the war in Ukraine drew our attention in this regard, and we agree with this opinion of climate researcher Ottmar Edenhofer:

It is misunderstood that the basic idea of free trade, multilateralism, and the spread of human rights leads to the fact that we live in a world in which, in essence, only democracies act with each other and shape international relations with each other, that is, in essence, the vision Kant wrote down in “*Zum ewigen Frieden*”²⁵⁹⁵. The focal point of world history is that we have to say goodbye to that. We live in a world where so-called “democracies” and “autocracies” are intertwined in an unholy way, and we still have to find a way to cooperate with the autocracies in a limited but nonetheless cooperative way.²⁵⁹⁶

²⁵⁹² NOYB. (10 July 2023). *New Trans-Atlantic Data Privacy Framework largely a copy of “Privacy Shield”*. *noyb will challenge the decision*. <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.

²⁵⁹³ Duball, J. [Joseph]. (3 September 2020). *LIBE meeting scrutinizes path forward for EU-US data transfers*. <https://iapp.org/news/a/libe-meeting-reveals-plan-scrutiny-of-path-forward-for-eu-us-data-transfers>.

²⁵⁹⁴ Greenleaf, G. [Graham]. (2014). *A World Data Privacy Treaty?* In *Emerging Challenges in Privacy Law*, Cambridge University Press. P. 93

²⁵⁹⁵ Kant, I. [Immanuel]. (1796). *Zum ewigen Frieden. Ein philosophischer Entwurf. Neue vermehrte Auflage*. Frankfurt und Leipzig.

²⁵⁹⁶ Dausend, P. [Peter] and Hildebrandt, T. [Tina]. (8 July 2022). *Der Krieg ist klimapolitisch ein Desaster*. In *Das Politikeil / Energiewende*. Zeit Online. https://www.zeit.de/politik/2022-07/energiewende-energiepolitik-ukraine-krieg-politikpodcast?utm_referrer=https%3A%2F%2Fwww.google.com%2F.

We do not want to leave unmentioned here another feature of the German legal area which has been adopted on the international political stage: The keyword of “*Realpolitik*”. We also think, with Atkinson / Cory, that

a pragmatic global digital economy strategy will require changes from everyone. The United States needs to move away from an idealist view of digital international relations to a *Realpolitik* one, which is focused more on protecting key economic interests rather than acting as a global ambassador of complete and unfettered Internet openness. Countries do and will continue to take differing approaches to moderating and blocking content online. Countries should develop clear, predictable, and non-discriminatory legal and administrative frameworks for all firms – both foreign and domestic – to use so that they know what online content is and is not illegal.²⁵⁹⁷

Realpolitik is also needed to reach an international agreement for TFPD. There has been a lot of discussion about digital security policy recently, but the quality of the discussion is not yet at the level it should be. This matter, which is crucial for a functioning digital society, is not yet sufficiently understood by society as a whole. This is because our understanding of security is still shaped by protective measures in a territorial world. Whereas the 20th century was about organizing and securing 1-to-n relationships, the 21st century is about structuring and securing n-to-n relationships now included in networks. If we lack understanding of security in such new structures, then this could lead us to seek security in measures where security cannot be found. On the contrary, these measures could endanger the integrity of our digital society.

What we need is a “*Digitale Realpolitik*” that looks at the actual rather than the perceived threats. A good example is the current development of AI. In July 2023, 1011 Germans surveyed²⁵⁹⁸ shared their perceivance of AI. 92% have heard of AI, 72% said it is difficult to assess what AI brings with it, 46% noted that no clear picture of AI emerges from the media, 58% found the term AI unappealing. Perceptions of this technology are therefore diffuse. This is in contrast to “networking”, “digitization” and “digitalization”²⁵⁹⁹, terms whose positive recognition has risen from 46% to 69% over the past eight years. The opportunities²⁶⁰⁰ of AI, but unfortunately especially its risks²⁶⁰¹, have received special attention in business and society. Despite the widespread lack of knowledge about the details of AI-driven innovations and the still underdeveloped recognition (only 21%) of AI relating to their own everyday lives, 48% of respondents expect serious effects on the economy, 44% on society, only 16% associate AI primarily with opportunities, while 34% fear AI could lead to a threat to humanity and 22% even consider extinction of humanity a realistic scenario. The greater the uncertainty, the broader the consensus (of 56%) that

²⁵⁹⁷ Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century*, (pp. 217–232). Springer. P. 229.

²⁵⁹⁸ Köcher, R. [Renate]. (27 July 2023). Diffuse Ängste. *Frankfurter Allgemeine Zeitung*. P. 8.

²⁵⁹⁹ Chapter I, Section I.1.

²⁶⁰⁰ “However, there are hardly any proposals on this in the AI Act, and we should see this as an opportunity. Forcing a rapidly developing technology into the rigid framework of a law is not the best way to strengthen Europe’s lack of competitiveness in this area. What Europe needs is courage. Courage to agree not to restrict innovations in their development, but merely to provide them with guard rails. In concrete terms, this means not expanding the scope of the AI Act even further and instead closely accompanying the development of generative AI - and preferably not just nationally or European-wide, but globally.” Wissing, V. [Volker]. (15 July 2023). KI braucht innovative Regulierung. *Frankfurter Allgemeine Zeitung*. P. 23.

²⁶⁰¹ “AI would give hackers new opportunities for attacks. Irrespective of this, there has been a general increase in cyber-attacks in Germany. This is happening at all levels, so it affects companies as well as government agencies, the BSI [German Federal Office for Information Security] chief said. There has been a shift toward profit-oriented attacks. The threat level is higher than ever. We are seeing an increasing number of vulnerabilities in software products that make cyber-attacks possible in the first place.” *Frankfurter Allgemeine Zeitung*. (17 July 2023). KI-Sicherheitslabel im Gespräch. P. 17. // “AI can eventually handle the mind-boggling amounts of data [in the financial market] better, and at least the mediocre fund managers will fall by the wayside.” Mohr, D. [Daniel]. (6 July 2023). KI besser als MSCI-World-ETF. *Frankfurter Allgemeine Zeitung*. P. 27.

the development and use of AI should be regulated by the State, but at the same time only 23% believe that effective regulation is possible.

Returning to the AI use case of “ChatGPT”,²⁶⁰² it is clear that some data protection concerns are misguided or not addressed by – existing or to-be-designed – thoughtful regulation while enabling technological innovation. To the extent that ChatGPT involves any personal data at all, the company using Open AI’s product can ensure transparency by complying with its information obligations under the GDPR. Nevertheless, there remains the understandable accusation that Open AI trained the underlying AI model with unlawfully collected personal data. However, the better arguments suggest that this accusation does not have an effect on the use case by companies in their own offerings. While the stochastic data sets derived from training the AI are used by the algorithm in the downstream step, this is unlikely to constitute further (besides training the AI) processing of these personal data in scope of the GDPR. In contrast, the end user data collected via the API is not used for training purposes. As a result, such AI use cases can be used in a data protection-compliant manner as long as the legal requirements exist and are appropriate for these cases.

These perceptions and even fears multiply with the complexity, that is, in our case, with a subject matter affecting the international level. It is therefore important to avoid an abstract message of a threat to data protection without appropriately assessing the regulatory level, so that we can succeed in securing our rapidly evolving digital society and translating issues that really matter, such as our fundamental right to data protection. This requires the ability in *Realpolitik* to distinguish between changeable and unchangeable structures, and the ability to recognize time phases when change is possible (as we think now should be the time). Such change was already addressed by *Machiavelli* in 1532 in “*Il Principe*”²⁶⁰³, probably the earliest and most famous work of *Realpolitik*. *Machiavelli* was trying to understand a new era – the emerging modern age. Likewise, we need to understand our new era of the digital society. *Machiavelli* thought from the perspective of a prince. In our opinion, such a strategic and predominantly, but not exclusively, top-down perspective, should be reassumed and actively shaped in the regulation of TFPD at the international level. In doing so, however, a distinction must be made – as *Machiavelli* did – between the possible and the utopian. *Digitale Realpolitik* and therefore also all those involved in the digital society must then endure the tension that exists between openness and security and that balancing both cannot occur overnight. Rather, it is a process, similar to the way the Internet has given our time a different logic, away from territory and toward process. All stakeholders, and in particular the legislature, are called upon to reflect quickly in detail on such process, to ensure that preconditions for regulation are not continuously changed by technological progress and that “the legislative is not overtaken within a blind spot”, to intelligently explore possibilities, to think in a stakeholder-interest-driven manner; and to take into account that technological progress in the last two decades has widened the gaps between social classes, a fact that receives remarkably little attention.²⁶⁰⁴ Only then can we as a society as a whole achieve the best possible for all of us affected by TFPD.

²⁶⁰² Chapter I, Section I.1.

²⁶⁰³ Machiavelli, N. [Niccolò]. (1532). *Il Principe*. Antonio Blado d’Asola.

²⁶⁰⁴ Köcher, R. [Renate]. (27 July 2023). Diffuse Ängste. *Süddeutsche Zeitung*.

ABBREVIATIONS AND ACRONYMS

2001 SDPC	European Commission. (15 June 2001). Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, 2001/497/EC, OJ L 181, 19–31.
2004 SDPC	European Commission. (29 December 2004). Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 2004/915/EC, 74–84.
2010 SDPC	European Commission. (5 February 2010). Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 2010/87, 5–18.
ACHPR	African Commission on Human and Peoples' Rights
ACLU	American Civil Liberties Union
ACTA	United States of America, Office of the United States Trade Representative. Anti-Counterfeiting Trade Agreement (ACTA), https://ustr.gov/acta , (1 October 2011).
Additional Protocol	Council of Europe. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, ETS No. 181, https://rm.coe.int/1680080626 , (8 November 2001).
ADPPA	United States of America. American Data Privacy and Protection Act, H.R. 8152 (117th), (21 July 2022).
AI	Artificial Intelligence
APAC	Asia-Pacific
APEC	Asia-Pacific Economic Cooperation
APEC Privacy Framework 2005	Asia-Pacific Economic Cooperation. APEC Privacy Framework 2005, https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf , (2005).
APEC Privacy Framework 2015	Asia-Pacific Economic Cooperation. APEC Privacy Framework 2015, https://www.apec.org/apecapi/publication/getfile?publicationId=42d9fa81-f683-46a8-858b-1cde61fdb8f8 , (August 2017).
API	Application Programming Interface
API Directive	Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6 August 2004, 24–27.
ASEAN	Association of Southeast Asian Nations
ASEAN CBDF	Association of Southeast Asian Nations, Cross Border Data Flows Mechanism.
ASEAN DMF	Association of Southeast Asian Nations, Data Management Framework.
ASEAN Framework on Personal Data Protection	Association of Southeast Asian Nations. Framework on personal data protection, https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf , (November 2016).
ASEAN MCC	Association of Southeast Asian Nations. ASEAN Model Contractual Clauses, https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf , (22 January 2021).
AU	African Union
AUP	Acceptable Use Policy
B2B	business-to-business
B2C	Business-to-Consumer
BBC	British Broadcasting Corporation
BCR	Binding Corporate Rules
BCR+	BCR plus additional measures
BKartA	Bundeskartellamt, German Federal Antitrust Office.
BND	Bundesnachrichtendienst, the Foreign Intelligence Service of Germany.

Budapest Convention	Council of Europe. Convention on Cybercrime, ETS No. 185, (1 July 2004).
C2C	Controller-to-Controller Scenario (Module 1 of the third-countries-set)
C2P	Controller-to-Processor Scenario (Module 2 of the third-countries-set)
CAC	Cyberspace Administration of the People's Republic of China
CAHDATA	Council of Europe. Ad Hoc Committee on Data Protection.
CBPR	Asia-Pacific Economic Cooperation, Cross Border Privacy Rules System, http://cbprs.org/documents , (November 2011).
CCC	Council of Europe. Convention on Cybercrime, ETS No. 185, (1 July 2004).
CCPA	California State. California Consumer Privacy Act 2018, Cal. Legis. Serv. Ch. 55 (A.B. 375).
CERN	European Organization for Nuclear Research
CETA	Comprehensive Economic Trade Agreement
Charter	Charter of fundamental rights of the European Union
CIA	US Central Intelligence Agency
CISG	United Nations Convention on Contracts for the International Sale of Goods
Civil Code	The National People's Congress of the People's Republic of China. Civil Code of the People's Republic of China, http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf , (28 May 2020).
CIX	Commercial Internet Node
CJEU	Court of Justice of the European Union
Cloud Act	United States of America. CLOUD Act, H.R.4943, (2018).
CNIL	Commission Nationale de l'Informatique et des Libertés (the French SA)
CoC	Codes of Conduct
CODA	United States of America. Control Our Data Act.
CoE	Council of Europe
CoE MCC	Council of Europe. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, Model Contractual Clauses for the Transfer of Personal Data, T-PD(2022)1rev8, (3 March 2023).
ColoPA	Colorado State. Act concerning additional protection of data relating to personal privacy, SB21-190, https://leg.colorado.gov/bills/sb21-190 , (8 July 2021).
Commission	European Commission
controller-processor-draft-set	European Commission. (2020). Data protection - standard contractual clauses between controllers & processors located in the EU (implementing act). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Data-protection-standard-contractual-clauses-between-controllers-processors-located-in-the-EU-implementing-act_en .
controller-processor-set	European Commission. Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, C/2021/3972, OJ L 199, 18–30, (7 June 2021).
Convention 108	Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 (28 January 1981).
Convention 108+	Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223, CETS No. 223 (10 October 2018).
COPPA	United States of America. Children's Online Privacy Protection Rule, 15 U.S.C. 6501-6508, (7 January 2013).
COPRA	United States of America. Consumer Online Privacy Rights Act, 116th Congress (2019-2020), S.2968.
Council	Council of the European Union
CPEA	Asia-Pacific Economic Cooperation. APEC Cross-border Privacy Enforcement Arrangement (CPEA), https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement , (September 2021).
CPPA	California Privacy Protection Agency
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership

CSL	The National People's Congress of the People's Republic of China. CCybersecurity Law of the People's Republic of China, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china , (7 November 2016).
CSP	Cloud Service Provider
CTDPA	Connecticut State. Act Concerning Personal Data Privacy and Online Monitoring, S.B. No. 6, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&whi ch_year=2022 , (10 May 2022).
Data Act	European Commission. Proposal for a Regulation of the European Parliament and the Council on harmonized rules on fair access to and use of data (Data Act), COM(2022) 68 final, (23 February 2022).
Data Strategy	European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data, COM(2020) 66 final, (19 February 2020).
Database Directive	European Commission. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 077, 20–28, (27 March 1996).
DGA	European Commission. Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act), COM(2020) 767 final, (25 November 2020).
Digital Markets Act	European Commission, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 1–66, (12 October 2022).
Digital Services Act	European Commission, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 1–102, (27.10.2022).
Digital Services Act Package	Includes the Digital Services Act and the Digital Markets Act.
Directive 95/46	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
DMA	European Commission, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 1–66, (12 October 2022).
DNI	US Director of National Intelligence
DPO	Data Protection Officer
DSA	European Commission, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 1–102, (27.10.2022).
DSL	The National People's Congress of the People's Republic of China. Data Security Law of the People's Republic of China, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml , (10 June 2021).
EC	European Community / European Communities
EC Treaty	European Communities. Treaty establishing the European Community (Consolidated version 2002), OJ C 325, 33–184, (24 December 2002).
ECD	European Communities. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal L 178, 1–16, (17 July 2000).
ECHR	European Convention on Human Rights
ECIPE	European Centre for International Political Economy
E-Commerce	Electronic Commerce
E-Commerce Directive	European Communities. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal L 178, 1–16, (17 July 2000)
ECPA	United States of America. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523.
ECTHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPB Recommendations 01/2020 (Version 1.0)	European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 1.0, (10 November 2020), https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf .

EDPB Recommendations 01/2020 (Version 2.0)	European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, (18 June 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf .
EDPB Recommendations 02/2020	European Data Protection Board. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, (10 November 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentianguaranteessurveillance_en.pdf . P. 7.
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights and Privacy International
EEA	European Economic Area
EEA Agreement	Agreement on the European Economic Area, OJ No L 1, 3 January 1994, https://www.efta.int/Legal-Text/EEA-Agreement-1327
E-Evidence Directive	European Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final - 2018/0107 (COD), (17 April 2018).
E-Evidence Package	Includes E-Evidence Regulation and E-Evidence Directive.
E-Evidence Regulation	European Commission. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD), (17 April 2018).
EFF	Electronic Frontier Foundation
EIO Directive	European Commission. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1–36, (1 May 2014).
ENISA	European Union Agency for Network and Information Security
EO	Executive Order
EO 12333	United States of America. Executive Order 12333, US Federal Register, 46 FR 59941, 3 CFR, 1981 Comp., P. 200 (4 December 1981).
EO 14086	United States of America, The White House. Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ , (7 October 2022).
EP	European Parliament
EPIC	Electronic Privacy Information Center
EPOC	European Production Order Certificate
EPOC-PR	European Preservation Order Certificate
E-Privacy Directive	European Communities. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 37–47, (31 July 2002).
E-Privacy Regulation	European Commission. Proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final, (10 January 2017).
EU	European Union
EUCS	Cybersecurity Certification Scheme for Cloud Services
EUCSA	European Commission. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 15–69, (7 June 2019).
EU-Japan MLAT	European Union. Agreement between the European Union and Japan on mutual legal assistance in criminal matters. OJ L 39, 20-35, (12 February 2010).
EUR	Euro (currency)
EURATOM	European Atomic Energy Community
EU-US DPF	EU-US Data Privacy Framework
EU-US MLAT	European Union. Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181, 34–40, (19 July 2003).
EU-US TFTP agreement	European Commission. Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 5–14, (27 July 2010).

Explanatory Report to Convention 108+	Council of Europe. Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 223, (10 October 2018).
Facebook fanpages case	Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd, C 210/16, ECLI:EU:C:2018:388.
FBI	US Federal Bureau of Investigation
FCC	United States of America, Federal Communications Commission.
FISA	United States of America. Foreign Intelligence Surveillance Act, 50 U.S.C. Paras. 1801–11, 1821–29, 1841–46, 1861–62, 1871, (1978).
FISC	United States Foreign Intelligence Surveillance Court
Freedom Act	United States of America. Public Law 114 - 23 - Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, H.R. 2048.
FTC	United States of America, Federal Trade Commission.
FTCA	United States of America. Federal Trade Commission Act, 15 U.S.C. §§ 41-58.
GA	General Assembly
GATS	World Trade Organization. General Agreement on Trade in Services, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm , (1995).
GATT	World Trade Organization. General Agreement on Tariffs and Trade 1994, https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm , (1994).
GBP	British pound sterling (currency)
GCHQ	United Kingdom, Government Communications Headquarters.
GDPR	European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Official Journal of the European Union L 119 (4 May 2016), 1–88.
GLBA	United States of America. Gramm-Leach-Bliley Act, 15 U.S.C. 6801-6809, (12 November 1999).
GNI	Global Network Initiative
Google Spain case	Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317.
GPEN	Organization for Economic Co-operation and Development, Global Privacy Enforcement Network.
IaaS	Infrastructure as a Service
IAGMR	Inter-American Court of Human Rights
IAPP	International Association of Privacy Professionals
IC	Intelligence Community
ICC	International Chamber of Commerce
ICCL	Irish Council on Civil Liberties
ICCPR	United Nations, Office of the High Commissioner for Human Rights. International Covenant on Civil and Political Rights, General Assembly resolution 2200A (XXI), (16 December 1966).
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICESR	United Nations, Office of the High Commissioner for Human Rights. International Covenant on Economic, Social and Cultural Rights, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx , (16 December 1966).
ICJ	International Court of Justice
ICO	Information Commissioner's Office
IEC	International Electrotechnical Commission
ILO	International Labor Organization
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IoT	Internet of Things
IPRED2	European Commission. Amended proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights, COM(2006) 168 final, (24 June 2006).
IRS	United States of America. Internal Revenue Service Rule, 26 U.S.C. § 7216, (1986).

ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
JR Act	United States of America. Judicial Redress Act of 2015, H.R. 1428 (114th), (24 February 2016).
La Quadrature du Net case	Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 6 October 2020, La Quadrature du Net and others v Conseil des ministers, ECLI:EU:C:2020:791.
LED	European Commission. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the European Union, L 119/89, (4 May 2016).
LIBE	European Parliament's Committee on Civil Liberties, Justice and Home Affairs
Ligue des droits humains case	Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 21 June 2022, Request for a preliminary ruling under Article 267 TFEU from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 17 October 2019, received at the Court on 31 October 2019, in the proceedings Ligue des droits humains v Conseil des ministers, Case C-817/19, ECLI:EU:C:2020:68.
Madrid Resolution	International Conference of Data Protection and Privacy Commissioners. The Madrid Resolution, https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf , (2009).
Member States	Member States of the European Union
MEP	Member of the European Parliament
Meta	Meta Platforms Inc.
Microsoft Ireland case	United States of America. Microsoft Corporation v. United States of America, 2d Cir., Case No. 14-2985, (14 July 2016).
MLAT	Mutual Legal Assistance Treaty
MNE	Multinational Enterprise
Montreux Declaration	International Conference of Data Protection and Privacy Commissioners. Montreux Declaration, https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf , (2005).
NAFTA	North American Free-Trade Area
NOYB	NOYB – European Center for Digital Rights
NSA	US National Security Agency
NSC	US National Security Council
NSF	National Science Foundation
NSL	National Security Letter
NTIA	US National Telecommunications and Information Administration
OCII	Operators of Critical Information Infrastructure
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-operation and Development
OECD Guidelines 1980	Organization for Economic Co-operation and Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.uio.no/studier/emner/jus/jus/JUTPRIV/h05/undervisningsmateriale/oecd-pv.doc , (23 September 1980),
OECD Guidelines 2013	Organization for Economic Co-operation and Development. Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf , (11 July 2013).
OECD Privacy Framework	Organization for Economic Co-operation and Development. The OECD Privacy Framework. (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf .
OJ	Official Journal
OPA	United States of America. Online Privacy Act of 2019, 116th Congress (2019-2020), H.R. 4978.
Open Data Directive	European Commission. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive), OJ L 172, 56–83, (26 June 2019).
OTT	Over-the-top content

P2B Regulation	European Commission. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 57–79, (11 July 2019).
P2C	Processor-to-Controller Scenario (Module 4 of the third-countries-set)
P2P	Processor-to-Processor Scenario (Module 3 of the third-countries-set)
PaaS	Platform as a Service
Parliament	European Parliament
Patriot Act	United States of America. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, H.R. 3162, Publ. L. No. 107–56, 115 Stat. 272, (26 October 2001).
PCLOB	United States Privacy and Civil Liberties Oversight Board
PETs	Privacy Enhancing Technologies
PI	Personal Information
PI Specification 2018	People's Republic of China, National Standard of Information Security Technology - Personal Information Security Specification.
PI Specification 2020	People's Republic of China, National Standard of Information Security Technology - Revised Personal Information Security Specification.
PII	Personally Identifiable Information
PIL	Private International Law
PIPA	United States of America. PROTECT IP Act of 2011, S.968 (112th), (26 May 2011).
PIPIA	Personal Information Protection Impact Assessment
PIPL	The National People's Congress of the People's Republic of China. Personal Information Protection Law of the People's Republic of China, Chairman's Order No. 91, (20 August 2021).
PIU	Passenger Information Unit
PNR	Passenger Name Records
PNR Directive	European Commission. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Official Journal of the European Union, L 119/132 (4 May 2016).
POTUS	President of the United States of America
PPD-28	United States of America, The White House. Presidential Policy Directive -- Signals Intelligence Activities, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities , (17 January 2014).
PRC	People's Republic of China
PRC Certification Specification	People's Republic of China. Information security technology-Certification requirements for cross-border transmission of personal information, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381 , (16 March 2023).
PRC Security Assessment Guidelines	People's Republic of China. Guidelines for Data Exit Security Assessment and Declaration (First Edition), http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm , (2022).
PRC Security Assessment Measures	People's Republic of China. Measures for Data Export Security Assessment, http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm , (1 September 2022).
PRC Standard Contract	People's Republic of China. Standard Contract Measures for the Export of Personal Information, http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm , (1 June 2023).
PRC Standard Contract Guidelines	People's Republic of China. Guidelines for the Filing of Standard Contracts for Exporting Personal Information Abroad (First Edition), http://www.cac.gov.cn/2023-05/30/c_1687090906222927.htm , (Mai 2023).
PRC Technical Specifications	People's Republic of China. Technical Specifications for Certification of Cross-Border Processing of Personal Information, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381 , (16 March 2023).
Privacy Act	United States of America. The Privacy Act of 1974, Public Law No. 93-579, 5 U.S.C. § 552 a.
RCEP	Association of Southeast Asian Nations. Regional Comprehensive Economic Partnership Agreement, https://rcepsec.org/legal-text , (1 January 2022).
Resolution 2013	United Nations, General Assembly. Resolution adopted by the General Assembly on 18 December 2013, A/RES/68/167, (18 December 2013).

Resolution 2021	United Nations, General Assembly. Resolution adopted by the Human Rights Council on 7 October 2021, A/HRC/RES/48/4, (13 October 2021).
RIA	Regulatory Impact Assessment
Rome I	European Communities. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177/6, (4 July 2008).
Rome II	European Union. Regulation (EU) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199/40, (31 July 2007).
RoPA	Records of Processing Activities
RPS	Regulatory Pilot Space
RUDs	Reservations, understandings, and declarations.
SA	Supervisory Authority
SaaS	Software as a Service
Safe Harbor	European Commission. (25 August 2000). Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. 2000/520/EC. OJ L 215, 7–47.
SCA	United States of America. Stored Communications Act, 18 U.S.C. Chapter 121, Paras. 2701–2713, (1986).
SCC	European Union, Standard Contractual Clauses; synonymous with SDPC.
Schrems I case	Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 6 October 2015, Maximilian Schrems v Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650.
Schrems II case	Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems, Case C-311/18, ECLI:EU:C:2020:559.
SDGs	UN's Sustainable Development Goals
SDPC	European Union, Standard Data Protection Clauses; synonymous with SCC.
SDPC+	SDPC plus additional measures
Set I	European Commission. (15 June 2001). Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, 2001/497/EC, OJ L 181, 19–31.
Set II	European Commission. (29 December 2004). Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 2004/915/EC, 74–84.
Set III	European Commission. (5 February 2010). Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 2010/87, 5–18.
SIS II	European Union. Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 4–23, (28 December 2006).
SME	Small and medium-sized enterprise
Solange I case	German Constitutional Court. Judgment. BVerfGE 37, 271 ff.
SOPA	United States of America. Stop Online Piracy Act, H.R. 3261 (112th), (26 October 2011).
SP	Service Provider
SSL	Secure Sockets Layer
Steel Seizure Case	United States of America. Youngstown Sheet & Tube Co. v. Sawyer, Supreme Court, 343 U.S. 579 (1952).
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEU	European Union. Consolidated version of the Treaty on European Union, Official Journal of the European Union, C 326/13, (26 October 2012)
TFEU	European Union. Consolidated version of the Treaty on the Functioning of the European Union, Official Journal of the European Union, C 326/47, (26 October 2012).
TFPD	Transborder Flow(s) of Personal Data
TFTP	Terrorist Finance Tracking Program.

TFTP Agreement	The Council of the European Union. 2010/412/: Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 3–4, (27 July 2010).
third-countries-draft-set	European Commission. (2020). Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act_en .
third-countries-set	European Commission. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C/2021/3701, OJ L 199, 31–61, (7 June 2021).
TIA	Transfer Impact Assessment
T-PD	Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
Treaty of Amsterdam	European Communities. Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ C 340, 1–144, (10 November 1997).
Treaty of Lisbon	European Union. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on European Union - Protocols - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, Official Journal of the European Union, C 326, 1–390, (signed on 13 December 2007, published 26 October 2012).
TRIPS	World Trade Organization. Agreement on Trade-Related Aspects of Intellectual Property Rights, https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm , (15 April 1994).
TTIP	Transatlantic Trade and Investment Partnership
UDHR	United Nations. Universal Declaration of Human Rights, https://www.un.org/sites/un2.un.org/files/udhr.pdf , (10 December 1948).
UK	United Kingdom
Umbrella Agreement	European Commission. Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ L 336, 3–13, (10 December 2016).
UN	United Nations
UN Charter	Charter of the United Nations
UN ECOSOC	United Nations, Economic and Social Council.
UN Guidelines	United Nations, General Assembly. Guidelines for the Regulation of Computerized Personal Data Files, Resolution 45/95, (14 December 1990).
UN HRC	United Nations Human Rights Council
UNCITRAL	United Nations, Commission on International Trade Law.
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations, Educational, Scientific and Cultural Organization.
UNIDROIT	International Institute for the Unification of Private Law
Union	European Union
US Constitution	United States of America. The Constitution of the United States, (4 March 1789).
USA	United States [of America]
USA	United States of America
USCDPA	Hunton Williams. United States Consumer Data Privacy Act of 2019. https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf .
USD	US Dollar (currency)
USMCA	US - Mexico - Canada Free Trade Agreement
VCDPA	Virginia State. Consumer Data Protection Act, SB 1392, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53 , (2 March 2021).
VCLT	United Nations. Vienna Convention on the Law of Treaties, United Nations Treaty Series, Vol. 1155, P. 331, (1969).
Verein für Konsumenteninformation case	Court of Justice of the European Union. Judgment of the Court of 28 July 2016, Verein für Konsumenteninformation v Amazon EU Sàrl, C-191/15, ECLI:EU:C:2016:612.
VIS	Visa database

VLOP	Very Large Online Platform
Warsaw Declaration	International Conference of Data Protection and Privacy Commissioners. Warsaw Declaration, https://icdppc.org/wp-content/uploads/2015/02/Warsaw-declaration-on-Application-of-society-EN.pdf , (2013).
WEF	World Economic Forum
Weltimmo case	Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 1 October 2015. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság. C-230/14, ECLI:EU:C:2015:639.
Wiretap Act	United States of America. Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351, Title III, (19 June 1968).
WP29	Article 29 Working Party
WTO	World Trade Organization
WTO JSI	World Trade Organization, Joint Statement Initiative on e-commerce.
WWW	World Wide Web

BIBLIOGRAPHY

1. Legislation, acts, guidelines

- African Commission on Human and Peoples' Rights. *African Charter on Human and Peoples' Rights*, (27 June 1981).
- Article 29 Data Protection Working Party. *Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten*, GD XVD/5047/98, WP 14, (30 November 1998).
- Article 29 Data Protection Working Party. *Joint statement of the European Data Protection Authorities assembled in the Article 29 Working Party*, WP 227, (26 November 2014).
- Article 29 Data Protection Working Party. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, WP 238, (13 April 2016).
- Article 29 Data Protection Working Party. *Opinion 4/2000 on the level of protection provided by the Safe Harbor Principles*, WP32, (16 May 2000).
- Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data*, WP 136, (2007).
- Article 29 Data Protection Working Party. *Statement on the decision of the European Commission on the EU-U.S. Privacy Shield*, https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf, (26 July 2016).
- Article 29 Data Protection Working Party. *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, GD XVD/5025/98, WP 12, (24 July 1998).
- Article 29 Data Protection Working Party. *Working Document 01/2009 on pre-trial discovery for cross border civil litigation*, WP 158, (11 February 2009).
- Article 29 Data Protection Working Party. *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP114, (25 November 2005).
- Article 29 Data Protection Working Party. *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, WP 256, (6 February 2018).
- Article 29 Working Party. *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*, WP 212, (27 February 2014).
- Asia-Pacific Economic Cooperation. *APEC Cross-border Privacy Enforcement Arrangement (CPEA)*, <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement>, (September 2021). ("CPEA").
- Asia-Pacific Economic Cooperation. *APEC Data Privacy Pathfinder*, 2007/CSOM/019.
- Asia-Pacific Economic Cooperation. *APEC Privacy Framework 2005*, https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf, (2005).
- Asia-Pacific Economic Cooperation. *APEC Privacy Framework 2015*, <https://www.apec.org/apecapi/publication/getfile?publicationId=42d9fa81-f683-46a8-858b-1cde61fdb8f8>, (August 2017).
- Asia-Pacific Economic Cooperation. *Cross Border Privacy Rules System*, <http://cbprs.org/documents>, (November 2011). ("CBPR").
- Asia-Pacific Economic Cooperation. *Regulations, Policies and Initiatives on E-Commerce and digital economy for APEC MSMEs' Participation in the Region*. https://www.apec.org/docs/default-source/publications/2020/3/regulations-policies-and-initiatives-on-e-commerce-and-digital-economy/220ecsgregulations-policies-and-initiatives-on-ecommerce-and-digital-economy-for-apec-msmes-particip.pdf?sfvrsn=63b748d7_1, (March 2020).
- Asia-Pacific Economic Cooperation. *What is the Cross-Border Privacy Rules System?*, <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System>, (15 April 2019).
- Association of Southeast Asian Nations and European Commission. *Joint guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*. <https://asean.org/wp-content/uploads/2023/05/The-Joint-Guide-to-ASEAN-Model-Contractual-Clauses-and-EU-Standard-Contractual-Clauses.pdf>, (2023).
- Association of Southeast Asian Nations. *ASEAN Data Management Framework*, https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf, (January 2021). ("ASEAN DMF").
- Association of Southeast Asian Nations. *ASEAN Framework on digital governance*. https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf.
- Association of Southeast Asian Nations. *ASEAN Model Contractual Clauses*, https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf, (22 January 2021). ("ASEAN MCC").

- Association of Southeast Asian Nations. *Framework on personal data protection*, <https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf>, (November 2016).
- Association of Southeast Asian Nations. *Regional Comprehensive Economic Partnership Agreement*, <https://rcepsec.org/legal-text>, (1 January 2022). ("RCEP").
- Australian Government, Department of Foreign Affairs and Trade. *CPTPP text and associated documents*, <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents>, (8 March 2018).
- Bundesland Hessen. *Datenschutzgesetz*, Gesetz- und Verordnungsblatt für das Land Hessen, 1 Y 3228 A, 625–627, (12 October 1970).
- California State. *California Consumer Privacy Act 2018*, Cal. Legis. Serv. Ch. 55 (A.B. 375). ("CCPA").
- California State. *California Online Privacy Protection Act of 2003, as amended by A.B. 370*, California Business & Professions Code Sec. 22575 - 22579 (2004), (11 January 2014). ("COPPA").
- California State. *California Privacy Rights Act of 2020 (CPRA), also known as Proposition 24*, https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5, (3 November 2020). ("CPRA").
- California State. *California Senate Bill no. 568 to add Chapter 22.1 (Sec. 22580 - 22582) to Division 8 of the Business and Professions Code*, (22 February 2013).
- California State. *Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment)*, https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf, (4 November 2019).
- Colorado State. *Act concerning additional protection of data relating to personal privacy*, SB21-190, <https://leg.colorado.gov/bills/sb21-190>, (8 July 2021). ("ColoPA").
- Commission Nationale Des Droits De l'Homme Et Des Liberté Chad. *Communication 4/92*, 9th ACHPR AAR Annex VIII (1995-1996).
- Commission of the European Communities. *Communication from the Commission to the Council and the European Parliament on european contract law*, COM/2001/0398 final, 15–18, (2001).
- Commission of the European Communities. *Communication from the Commission to the European Parliament and the Council - A more coherent European contract law - An action plan*, Official Journal of the European Union C 63/1, (2003).
- Commission of the European Communities. *Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data*, Procedure 1990/0287/COD, COM (1990) 314 - 2, (18 July 1990).
- Connecticut State. *Act Concerning Personal Data Privacy and Online Monitoring*, S.B. No. 6, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022, (10 May 2022). ("CTDPA").
- Council of Europe. *128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018), Ad hoc Committee on Data Protection (CAHDATA) – Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), CM(2018)2-final*, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e, (18 May 2018).
- Council of Europe. *20th meeting of the Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, T-PD-BUR (2010) RAP 20, (16 March 2010).
- Council of Europe. *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*, ETS No. 181, <https://rm.coe.int/1680080626>, (8 November 2001).
- Council of Europe. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)*, ETS No. 189, (1 March 2006).
- Council of Europe. *Amendments approved by the Committee of Ministers, in Strasbourg, on 15 June 1999*, <https://rm.coe.int/168008c2b8>, (15 June 1999).
- Council of Europe. *Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, Model Contractual Clauses for the Transfer of Personal Data*, T-PD(2022)1rev8, (3 March 2023). ("CoE MCC").
- Council of Europe. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223*, CETS No. 223 (10 October 2018). ("Convention 108+"),
- Council of Europe. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS No. 108 (28 January 1981). ("Convention 108").
- Council of Europe. *Convention on Cybercrime*, ETS No. 185, (1 July 2004). ("CCC").
- Council of Europe. *Draft explanatory report – Convention 108 modernized*, <https://rm.coe.int/16806b6ec2>, (24 August 2016).
- Council of Europe. *Draft modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, GR-J(2016)1, (September 2016).
- Council of Europe. *European Convention on Human Rights*, CETS 005, (4 November 1950). ("ECHR")
- Council of Europe. *Explanatory report to the Convention on Cybercrime*, (8 November 2001)
- Council of Europe. *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. CETS No. 223, (10 October 2018).

- Council of Europe. *Information Document*, CAHDATA(2013) Inf, (17 September 2013).
- Council of Europe. *Joint statement by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe*, <https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb>, (7 September 2020).
- Council of Europe. *Memorandum of Understanding between the Council of Europe and the European Union*, <https://rm.coe.int/1680597b32>, (23 May 2007).
- Council of Europe. *Protocol No. 11 to the Convention for the protection of human rights and fundamental freedoms, restructuring the control machinery established thereby*, ETS 155, (11 May 1994).
- Council of Europe. *Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention*, Treaty No.194, (13 May 2004).
- Council of Europe. *Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods*, (9 November 2011).
- Council of Europe. *Resolution No. 3 on data protection and privacy in the third millennium*, MJU-30 (2010) RESOL. 3, (26 November 2010).
- Council of Europe. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, CM(2021)57-final, (17 November 2021).
- Council of Europe. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Explanatory Report*, CM(2021)57-addfinal, (17 November 2021).
- Council of Europe. *Statute of the Council of Europe*, ETS No. 001, (5 May 1949).
- Council of Europe. *Transborder access to data and jurisdiction: Options for further action by the T-C, T-CY* (2014)16, (3 December 2014).
- Council of the EU. *Council position and findings on the application of the General Data Protection Regulation (GDPR)*, ST 14994/2/19, Rev. 2, <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/en/pdf>, (15 January 2020).
- Council of the EU. *Draft Directives for the negotiation of a plurilateral agreement on trade in services*, <https://data.consilium.europa.eu/doc/document/ST-6891-2013-ADD-1-DCL-1/en/pdf>, (10 March 2015).
- Council of the EU. *EU-US summit statement: Towards a renewed Transatlantic partnership*. <https://www.consilium.europa.eu/media/50758/eu-us-summit-joint-statement-15-june-final-final.pdf>. (15 June 2021).
- Council of the EU. *Preparation of the Council position on the evaluation and review of the GDPR – Comments from Member States*, ST 12756/1/19, <https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf>, (9 October 2019).
- Council of the European Union. *2010/412/ Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, OJ L 195, 3–4, (27 July 2010). (“TFTP”).
- Council of the European Union. *Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, OJ C 197, 1–2, (12 July 2000).
- Council of the European Union. *Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data*, OJ L 261, 24–27, (6 August 2004).
- Council of the European Union. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Presidency discussion paper*, 2017/0003(COD), (6 July 2020).
- Council of the European Union. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Presidency discussion paper*, 6 March 2020, 2017/0003(COD), available at <https://data.consilium.europa.eu/doc/document/ST-6543-2020-INIT/en/pdf>, (8 October 2021).
- Datatilsynet. *Ny aftale om udveksling af personoplysninger mellem EU og USA*, <https://www.datatilsynet.dk/internationalt/internationalt-nyt/2022/mar/ny-aftale-om-udveksling-af-personoplysninger-mellem-eu-og-usa>, (29 March 2022).
- Deutscher Bundestag. *Antwort der Bundesregierung*, Drucksache 19/21077, (14 July 2020).
- European Commission, *Proposal for a decision authorising Member States to sign, in the interest of the European Union, the Protocol of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, COM(2018) 449 final, (5 June 2018).
- European Commission, *Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, COM/2018/226 final - 2018/0107 (COD), (17 April 2018). (“E-Evidence Directive”).
- European Commission, *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*, OJ L 265, 1–66, (12 October 2022). (“Digital Markets Act”).
- European Commission, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, OJ L 277, 1–102, (27.10.2022). (“Digital Services Act”).

- European Commission. (5 June 2020). *Inception Impact Assessment*, Ref. Ares(2020)2916519.
- European Commission. (February 2020). *Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data Final Report*. <https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF>.
- European Commission. *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, (6 May 2015).
- European Commission. *A new EU-US agenda for global change*, JOIN(2020) 22 final, (2 December 2020).
- European Commission. *Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service*, OJ L 186, 4–16, (14 July 2012).
- European Commission. *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, OJ L 195, 5–14, (27 July 2010). (“EU-US TFTP agreement”).
- European Commission. *Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)*, OJ L 204, 16–25, (4 August 2007).
- European Commission. *Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences*, OJ L 336, 3–13, (10 December 2016).
- European Commission. *Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security*, *Official Journal of the European Union*, L 215, 5–14, (11 August 2012).
- European Commission. *Amended proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights*, COM(2006) 168 final, (24 June 2006).
- European Commission. *Better Regulation – joining forces to make better laws*, COM(2021)219, (2021).
- European Commission. *Better Regulation Guidelines*, SWD(2021) 305 final, (2021).
- European Commission. *Better regulation toolbox - November 2021 edition*. https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=br_toolbox-nov_2021_en.pdf, (2021).
- European Commission. *Better regulation: guidelines and toolbox*. https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en, (2021).
- European Commission. *Building a European Data Economy*, COM(2017) 9 final, (10 January 2017)
- European Commission. *Commission communication on the exchange and protection of personal data in a globalized world*, COM(2017) 7 final, (10 January 2017).
- European Commission. *Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information*, OJ L 76, 1–58, (19 March 2019).
- European Commission. *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, C/2021/3701, OJ L 199, 31–61, (7 June 2021). (“third-countries-set”).
- European Commission. *Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council*, C/2021/3972, OJ L 199, 18–30, (7 June 2021). (“controller-processor-set”).
- European Commission. *Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, OJ L 44, 1–90, (24 February 2022).
- European Commission. *Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, SWD(2020)128 final, (24 July 2020).
- European Commission. *Commission Staff Working Document, Impact Assessment, Accompanying the document Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol’s cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol’s role on research and innovation*, SWD/2020/543 final, (9 December 2020).
- European Commission. *Commission Staff Working Document, Impact Assessment, Accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118 final, (17 April 2018).
- European Commission. *Commission Staff Working Document, Impact Assessment, Accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council*

- laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118 final, (17 April 2018).
- European Commission. *Commission Staff Working Document. Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union*, SWD(2017) 304 final, (13 September 2017).
- European Commission. *Commission statement regarding the EU/US Agreement on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses ("Umbrella Agreement")*, OJ L 25, (31 January 2017).
- European Commission. *Commission statement regarding the EU/US Agreement on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses ("Umbrella Agreement")*, OJ L 25/2, (31 July 2017).
- European Commission. *Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries*, COM(2010) 492, (24 September 2010).
- European Commission. *Communication from the Commission to the European Parliament and the Council – The external dimension of the EU policy on Passenger Name Records*, Ref. Ares(2020)3918953.
- European Commission. *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14*, COM(2015) 566 final, (6 November 2015).
- European Commission. *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, (24 June 2020).
- European Commission. *Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalized World*, COM(2017) 7 final, (10 January 2011).
- European Commission. *Communication from the Commission to the European Parliament and the Council, Way forward on aligning the former third pillar acquis with data protection rules*, COM(2020) 262 final, (25 June 2020).
- European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data*, COM(2020) 66 final, (19 February 2020). ("Data Strategy").
- European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, COM(2012) 9 final, (25 January 2012).
- European Commission. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, Official Journal of the European Union, L 119/89, (4 May 2016). ("LED").
- European Commission. *Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Official Journal of the European Union, L 119/132 (4 May 2016). ("PNR Directive").
- European Commission. *Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive)*, OJ L 172, 56–83, (26 June 2019). ("Open Data Directive").
- European Commission. *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters*, OJ L 130, 1–36, (1 May 2014). ("EIO Directive").
- European Commission. *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases*, OJ L 077, 20–28, (27 March 1996). ("Database Directive").
- European Commission. *Directive of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC*, L 283/1, (10 October 2010).
- European Commission. *Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, Document Ares(2020)6654429.
- European Commission. *EU-US Trade and Technology Council: Commission launches consultation platform for stakeholder's involvement to shape transatlantic cooperation*, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_5308, (18 October 2021).
- European Commission. *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo*, https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443, (25 March 2021).
- European Commission. *Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, SWD(2019) 301 final, (22 July 2019).
- European Commission. *Notice concerning the provisional application of the Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union and its Member States, of the other part*, OJ L 238/9. (16 September 2017).
- European Commission. *Proposal for a Council Decision on the signing on behalf of the European Union of the Comprehensive Economic and Trade Agreement between Canada of the one part, and the European Union and its Member States, of the other part*, COM(2016)444, (5 July 2016).

- European Commission. *Proposal for a Directive of the European Parliament and of the Council amending Directive 2014/41/EU, as regards its alignment with EU rules on the protection of personal data*, 2021/0009 (COD), (20 January 2021).
- European Commission. *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011)32, (8 February 2011).
- European Commission. *Proposal for a Regulation of the European Commission and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, COM(2020) 825 final, (16 December 2020).
- European Commission. *Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679*, COM(2023) 348 final, (4 July 2023).
- European Commission. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final - 2018/0108 (COD), (17 April 2018). ("E-Evidence Regulation").
- European Commission. *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation*, COM(2020) 796 final, (9 December 2020).
- European Commission. *Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM(2017) 10 final, (10 January 2017). ("E-Privacy Regulation").
- European Commission. *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, COM(2020) 842 final, (15 December 2020).
- European Commission. *Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union*, COM/2022/119 final, Procedure 2022/0084/COD, (22 March 2022).
- European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, 2022/0140(COD), (3 May 2022).
- European Commission. *Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, COM(2020) 767 final, (25 November 2020). ("DGA").
- European Commission. *Proposal for a Regulation of the European Parliament and the Council on harmonized rules on fair access to and use of data (Data Act)*, COM(2022) 68 final, (23 February 2022). ("Data Act").
- European Commission. *Recommendation for a Council Decision authorizing the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, COM(2019) 70 final, (5 February 2019).
- European Commission. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, Official Journal of the European Union L 119 (4 May 2016), 1–88. ("GDPR").
- European Commission. *Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA*, OJ L 135, 53–114, (24 May 2016).
- European Commission. *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*, Official Journal of the European Union, L 295/39, (2018).
- European Commission. *Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services*, OJ L 186, 57–79, (11 July 2019). ("P2B Regulation").
- European Commission. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, OJ L 151, 15–69, (7 June 2019). ("EUCSA").
- European Commission. *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield*, COM(2017) 611 final.
- European Commission. *Report from the Commission to the European Parliament and the Council relating to Article 7(a) of Council Regulation (EC) No 2271/96 ('Blocking Statute')*, COM(2021) 535 final, (3 September 2021).
- European Commission. *Trade for All Towards a more responsible trade and investment policy*, COM (2015) 497 final, (14 October 2015).
- European Communities. *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, Official Journal L 178, 1–16, (17 July 2000). ("ECD" or "E-Commerce Directive").
- European Communities. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*

- (*Directive on privacy and electronic communications*), Official Journal L 201, 37–47, (31 July 2002). (“E-Privacy Directive”).
- European Communities. *Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)*, OJ L 177/6, (4 July 2008).
- European Communities. *Treaty establishing the European Community (Consolidated version 2002)*, OJ C 325, 33–184, (24 December 2002).
- European Communities. *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts*, OJ C 340, 1–144, (10 November 1997). (“Treaty of Amsterdam”).
- European Data Protection Board. (14 March 2022). *Guidelines 02/2022 on the application of Article 60 GDPR*. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022022-application-article-60-gdpr_en.
- European Data Protection Board. (20 October 2020). *EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679*. https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en.
- European Data Protection Board. *Adopted Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, (4 June 2019).
- European Data Protection Board. *Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection*, OUT2019-0007, (10 July 2019).
- European Data Protection Board. *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, (12 July 2022).
- European Data Protection Board. *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf. (14 January 2021).
- European Data Protection Board. *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, (19 November 2021).
- European Data Protection Board. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, (25 May 2018).
- European Data Protection Board. *Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransfers_publicbodies_v2_en.pdf, (15 December 2020).
- European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation*. (12 November 2019).
- European Data Protection Board. *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)*, (14 December 2018).
- European Data Protection Board. *Letter of 22 January 2021, OUT2021-0004*. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letteronreviewpnrdirective.pdf. (22 January 2021).
- European Data Protection Board. *Letter with Ref. OUT2020-0131*, https://edpb.europa.eu/sites/edpb/files/files/file1/out2020-0131_reply_letter_on_tftpagreement.pdf, (3 December 2020).
- European Data Protection Board. *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, (12 March 2019).
- European Data Protection Board. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 1.0*, (10 November 2020), https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasuretransferstools_en.pdf. (“EDPB Recommendation 01/2020 (Version 1.0)”).
- European Data Protection Board. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0*, (18 June 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasuretransferstools_en.pdf. (“EDPB Recommendation 01/2020 (Version 2.0)”).
- European Data Protection Board. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, (10 November 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanesentialguaranteessurveillance_en.pdf.
- European Data Protection Board. *Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)*, https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_en, (2 February 2021). P. 3.
- European Data Protection Board. *Statement 04/2021 on international agreements including transfers*, https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf, (13 April 2021).
- European Data Protection Board. *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf, (19 May 2021).

- European Data Protection Supervisor. *Case number: 2018-0638*, https://edps.europa.eu/sites/edp/files/publication/19-05-28_edps_inspection_report_art4_tftp_en.pdf, (28 May 2019)
- European Data Protection Supervisor. *EDPB Strategy 2021-2023*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_strategy2021-2023_en.pdf, (15 December 2020).
- European Data Protection Supervisor. *EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters*, Opinion 7/2019, https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf, (6 November 2019).
- European Data Protection Supervisor. *EUDPR: Conditions and Safeguards in International Transfers to Private Entities*, https://edps.europa.eu/system/files_en?file=2022-04/0167_2021-1047_01_redacted.pdf, (14 September 2021).
- European Data Protection Supervisor. *Guidelines 05/2020 on consent under Regulation 2016/679*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, (4 May 2020).
- European Data Protection Supervisor. *Opinion on the EU-U.S. Privacy Shield draft adequacy decision*, Opinion 4/2016, https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf, (30 May 2016).
- European Data Protection Supervisor. *Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence*, Opinion 2/2019, https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf, (2 April 2019).
- European Data Protection Supervisor. *Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, Opinion 1/2016, https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf, (12 February 2016).
- European Data Protection Supervisor. *Resolution on Cooperation with the UN Special Rapporteur on the Right to Privacy*, https://edps.europa.eu/sites/edp/files/publication/15-10-27_cooperation_un_special_rapporteur_en.pdf, (28 October 2015).
- European Economic Area. (3 January 1994). *Agreement on the European Economic Area*, OJ No L 1, <https://www.efta.int/Legal-Text/EEA-Agreement-1327>.
- European Parliament, European Council, European Commission. (31 December 2003). *Interinstitutional agreement on better law-making*, OJ C 321.
- European Parliament, *Legal Service*, *Opinion of 14 January 2016*, SJ-0784/15, (14 January 2016).
- European Parliament. (13 June 2023). *Electronic evidence: new rules to speed up cross-border criminal investigations*. https://www.europarl.europa.eu/pdfs/news/expert/2023/6/press_release/20230609IPR96203/20230609IPR96203_en.pdf.
- European Parliament. *Adequacy of the protection afforded by the EU-US Privacy Shield*, 2016/3018(RSP), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0131_EN.html, (6 April 2017).
- European Parliament. *An assessment of the Commission's proposals on electronic evidence*, PE 604.989, (September 2018), [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU\(2018\)604989_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf).
- European Parliament. *European Parliament resolution on the Commission's annual legislative programme for 2000*, Official Journal of the European Communities, C 377/323, (2000).
- European Parliament. *Legislative resolution of 1 December 2016 on the draft Council decision on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses*, 2016/0126(NLE), (1 December 2016).
- European Parliament. *Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD), (11 December 2020).
- European Parliament. *Resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP)*, (2014/2228(INI)), P8 TA(2015)0252.
- European Parliament. *Sunset Clauses in International Law and their Consequences for EU Law*, PE 703.592, [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703592/IPOL_STU\(2022\)703592_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703592/IPOL_STU(2022)703592_EN.pdf), (4 January 2022).
- European Union. *Agreement between the European Union and Japan on mutual legal assistance in criminal matters*. OJ L 39, 20-35, (12 February 2010). ("EU-Japan MLAT").
- European Union. *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program*, OJ L 195, 5-14, (27 July 2010).
- European Union. *Agreement on mutual legal assistance between the European Union and the United States of America*, OJ L 181, 34-40, (19 July 2003). ("EU-US MLAT").
- European Union. *Charter of fundamental rights of the European Union*, Official Journal of the European Union C 326 (26 October 2012), 391-407. ("Charter").
- European Union. *Consolidated version of the Treaty establishing the European Atomic Energy Community*, OJ C 327, 26.10.2012, 1-107, (26 October 2012).
- European Union. *Consolidated version of the Treaty on European Union*, Official Journal of the European Union, C 326/13, (26 October 2012). ("TEU" or "Treaty of Maastricht")

- European Union. *Consolidated version of the Treaty on the Functioning of the European Union*, Official Journal of the European Union, C 326/47, (26 October 2012). (“TFEU”).
- European Union. *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on European Union - Protocols - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon*, Official Journal of the European Union, C 326, 1–390, (signed on 13 December 2007, published 26 October 2012).
- European Union. *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws*, Official Journal of the European Union, L 337, (18 December 2009).
- European Union. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal of the European Union L 281 (23 November 1995), 31–50. (“Directive 95/46”).
- European Union. *Introduction to the EU Charter of fundamental rights*, C 303/17, (14 December 2007).
- European Union. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM(2021) 206 final (21 April 2021).
- European Union. *Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)*, OJ L 381, 4–23, (28 December 2006).
- European Union. *Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)*, OJ L 218, 60–81, (13 August 2008).
- European Union. *Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011*, OJ L 327, 20–82, (9 December 2017).
- European Union. *Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters*, OJ L 351/1, (20 December 2012).
- European Union. *Regulation (EU) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II)*, OJ L 199/40, (31 July 2007).
- Federal Republic of Germany. *Constitution for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III*, classification number 100-1, Federal Law Gazette I p. 968, (28 June 2022). (“Grundgesetz”).
- Federal Republic of Germany. *Introductory Act to the German Civil Code*, BGBl. I p. 3515, (10 August 2021). (“EGBGB”).
- Federal Republic of Germany. *Telemediengesetz of 26 February 2007 (BGBl. I p. 179, 251), as last amended 12 August 2021 (BGBl. I p. 3544)*. (26 February 2007).
- Inter-American Specialized Conference on Human Rights. *American Convention on human rights*, (22 November 1969).
- International Committee of the Red Cross. *The Geneva Conventions and their Commentaries*, (1949), <https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions>.
- International Conference of Data Protection and Privacy Commissioners. (29 October 2010). *Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data*. https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolution_international_en.pdf.
- International Conference of Data Protection and Privacy Commissioners. (29 September 2017). *Resolution on exploring future options for International Enforcement Cooperation (2017)*. <https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-exploring-future-options-for-International-Enforcement-Cooperation-2017.pdf>.
- International Conference of Data Protection and Privacy Commissioners. (5 November 2009). *International Standards on the Protection of Personal Data and Privacy, The Madrid Resolution*. https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf. (“Madrid Resolution”).
- International Conference of Data Protection and Privacy Commissioners. *Montreux Declaration*, https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf, (2005). (“Montreux Declaration”).
- International Conference of Data Protection and Privacy Commissioners. *The Madrid Resolution*, https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf, (2009). (“Madrid Resolution”).
- International Conference of Data Protection and Privacy Commissioners. *Warsaw Declaration*, <https://icdppc.org/wp-content/uploads/2015/02/Warsaw-declaration-on-Application-of-society-EN.pdf>, (2005). (“Warsaw Declaration”).
- International Court of Justice. *Statute of the International Court of Justice*, <https://www.icj-cij.org/en/statute>, (1945).

- International Labor Organization. *ILO Constitution*, https://www.ilo.org/dyn/normlex/en/f?p=1000:62:0::NO:62:P62_LIST_ENTRIE_ID:2453907:NO, (8 October 2015).
- Ministry of Commerce of the People's Republic of China. *MOFCOM Order No. 1 of 2021 on Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures*, <http://english.mofcom.gov.cn/article/policyrelease/announcement/202101/20210103029708.shtml>, (9 January 2021).
- Organization for Economic Co-operation and Development. *Action Plan for the Global Privacy Enforcement Network (GPEN)*, <https://www.privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen>, (15 June 2012).
- Organization for Economic Co-operation and Development. *Declaration on Transborder Data Flows*, https://www.oecd.org/document/32/0,3343,en_2649_34255_1888153_1_1_1_1,00.html, (11 April 1985).
- Organization for Economic Co-operation and Development. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/Final, <https://www.uio.no/studier/emner/jus/jus/JUTPRIV/h05/undervisningsmateriale/oecd-pv.doc>, (23 September 1980). ("OECD Guidelines 1980").
- Organization for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum*, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#preface>.
- Organization for Economic Co-operation and Development. *Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>, (11 July 2013). ("OECD Guidelines 2013").
- Organization for Economic Co-operation and Development. *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352>, (6 December 2007).
- Organization for Economic Co-operation and Development. *Recommendation of the Council on Regulatory Policy and Governance, (2012)*, <https://www.oecd.org/governance/regulatory-policy/2012-recommendation.htm>.
- Organization for Economic Co-operation and Development. *The OECD Privacy Framework*, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (2013). ("OECD Privacy Framework").
- Organization for Economic Co-operation and Development. *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL, [https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP\(2018\)19/FINAL&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/FINAL&docLanguage=En), (21 December 2018).
- People's Republic of China. *Cybersecurity Standards Practical Guide – Security Certification Specifications for Cross-Border Processing of Personal Information V2.0*, (16 December 2022).
- People's Republic of China. *GB/T 35273-2020*, <https://web.archive.org/web/20201124083428/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>, (6 March 2020).
- People's Republic of China. *Guidelines for Data Exit Security Assessment and Declaration (First Edition)*, http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm, (2022). ("PRC Security Assessment Guidelines").
- People's Republic of China. *Guidelines for the Filing of Standard Contracts for Exporting Personal Information Abroad (First Edition)*, http://www.cac.gov.cn/2023-05/30/c_1687090906222927.htm, (Mai 2023). ("PRC Standard Contract Guidelines").
- People's Republic of China. *Information security technology-Certification requirements for cross-border transmission of personal information*, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381, (16 March 2023). ("PRC Certification Specification").
- People's Republic of China. *Measures for Data Export Security Assessment*, http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm, (1 September 2022). ("PRC Security Assessment Measures").
- People's Republic of China. *Standard Contract Measures for the Export of Personal Information*, http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm, (1 June 2023). ("PRC Standard Contract").
- People's Republic of China. *State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020)*, <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020>.
- People's Republic of China. *Technical Specifications for Certification of Cross-Border Processing of Personal Information*, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381, (16 March 2023). ("PRC Technical Specifications").
- Russian Federation, State Duma. *Federal Law No. 152-FZ of 27 July 2006 On Personal Data*, https://wko.at/ooe/Branchen/Industrie/Zusendungen/FEDERAL_LAW.pdf, (27 July 2006).
- Russian Federation, State Duma. *Federal Law No. 242-FZ of 21 July 2014 Amending Certain Legislative Acts of the Russian Federation as to the Clarification of the Processing of Personal Data in Information and Telecommunications Networks*, <https://wilmap.stanford.edu/entries/federal-law-no-242-fz>, (21 July 2014).
- United Nations, Conference on Trade and Development. *Data protection regulations and international data flows: Implications for trade and development*, UNCTAD/WEB/DTL/STICT/2016/1/iPub, (2016).
- United Nations, Conference on Trade and Development. *Rising Product Digitalization and Losing Trade Competitiveness*, UNCTAD/GDS/ECIDC/2017/3, (2017).

- United Nations, General Assembly. *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, Resolution 2625, (24 October 1970).
- United Nations, General Assembly. *Doc. A/2929*, (1 July 1955).
- United Nations, General Assembly. *Guidelines for the Regulation of Computerized Personal Data Files*, Resolution 45/95, (14 December 1990).
- United Nations, General Assembly. *Human rights and scientific and technological developments*, Resolution 2450 of 19 December 1968, E/CN.4/1025, (19 December 1968).
- United Nations, General Assembly. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40, (17 April 2013).
- United Nations, General Assembly. *Resolution adopted by the General Assembly on 18 December 2013*, A/RES/68/167, (18 December 2013).
- United Nations, General Assembly. *Resolution adopted by the Human Rights Council on 7 October 2021*, A/HRC/RES/48/4, (13 October 2021). ("Resolution 2021").
- United Nations, General Assembly. *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/32/L.20, (27 June 2016).
- United Nations, Human Rights Committee. *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation*, <https://www.refworld.org/docid/453883f922.html>, (8 April 1988).
- United Nations, Human Rights Committee. *Comments on United States of America*, CCPR/C/79/Add 50, (1995).
- United Nations, Human Rights Committee. *Consideration of reports submitted by States parties under article 40 of the Covenant*, CCPR/C/ISR/CO/3, (2010).
- United Nations, Human Rights Committee. *General Comment No. 31 (80). The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add.13, (26 May 2004).
- United Nations, Human Rights Committee. *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie*, A/HRC/17/31, (21 March 2011).
- United Nations, Human Rights Committee. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, (30 June 2014).
- United Nations, Human Rights Committee. *Vienna Declaration and Programme of Action*, <https://www.ohchr.org/sites/default/files/vienna.pdf>, (25 June 1993).
- United Nations, Human Rights Council. *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, (30 June 2014).
- United Nations, Office of the High Commissioner for Human Rights. *Arab Charter on Human Rights*, <https://digitallibrary.un.org/record/551368>, (2004).
- United Nations, Office of the High Commissioner for Human Rights. *International Covenant on Civil and Political Rights*, General Assembly resolution 2200A (XXI), (16 December 1966).
- United Nations, Office of the High Commissioner for Human Rights. *International Covenant on Economic, Social and Cultural Rights*, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>, (16 December 1966).
- United Nations, Office of the High Commissioner for Human Rights. *Special Rapporteur on the right to privacy presents Draft Legal Instrument on Government-led Surveillance and Privacy*, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf, (28 February 2018).
- United Nations, Office of the High Commissioner for Human Rights. *State Responsibilities to Regulate and Adjudicate Corporate Activities under the United Nations' core Human Rights Treaties*, <https://media.business-humanrights.org/media/documents/files/reports-and-materials/Ruggie-ICCPR-Jun-2007.pdf>, (June 2007).
- United Nations, Office of the High Commissioner for Human Rights. *The right to privacy in the digital age: report (2021)*, A/HRC/48/31, (13 September 2021).
- United Nations. *Charter of the United Nations and Statute of the International Court of Justice*, (1945). ("UN Charter").
- United Nations. *Compilation of General Comments and General Recommendations adopted by human rights treaty bodies*, HRI/GEN/1/Rev.1, (29 July 1994).
- United Nations. UN Security Council, *Resolution 2178*, (2014).
- United Nations. United Nations Convention on Contracts for the International Sale of Goods, (1980). ("CISG").
- United Nations. *Universal Declaration of Human Rights*, <https://www.un.org/sites/un2.un.org/files/udhr.pdf>, (10 December 1948).
- United Nations. *Vienna Convention on the Law of Treaties*, United Nations Treaty Series, Vol. 1155, P. 331, (1969). ("VCLT")
- United States of America, Congressional Research Service. *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, R46724, (17 March 2021).
- United States of America, Congressional Research Service. *Federal Preemption: A Legal Primer*, R45825, (23 July 2019).
- United States of America, Congressional Research Service. *Overview of the American Data Privacy and Protection Act, H.R. 8152*, LSB10776, (31 August 2022).

- United States of America, Congressional Research Service. *U.S.-EU Privacy Shield and Transatlantic Data Flows*, R46917, (22 September 2021).
- United States of America, Department of Commerce. *EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>, (12 April 2023). (“Privacy Shield”).
- United States of America, Department of Commerce. *Global Cross-Border Privacy Rules Declaration*, <https://www.commerce.gov/global-cross-border-privacy-rules-declaration>, (2022).
- United States of America, Department of Commerce. *Global-Cross-Border-Privacy-Rules-Declaration-FAQ*, <https://www.commerce.gov/sites/default/files/2022-04/Global-Cross-Border-Privacy-Rules-Declaration-FAQ.pdf>, (2022).
- United States of America, Department of Justice, Office of the Attorney General. *Designation Pursuant to Section 3(f) of Executive Order 14086, 205-30*, (30 June 2023).
- United States of America, Department of Justice. *Justice Manual*, 9-47.120 - FCPA Corporate Enforcement Policy, § 9-47.120, <https://www.justice.gov/jm/jm-9-47000-foreign-corrup-practices-act-1977>, (2022).
- United States of America, Department of Justice. *Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086*, <https://www.justice.gov/d9/2023-07/Supporting%20Memorandum%20for%20the%20Attorney%20General%27s%20designation%20of%20EU-EEA.pdf>, (20 June 2023).
- United States of America, Federal Trade Commission. *FTC Policy Statement on Deception*, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf, (14 October 1983).
- United States of America, Federal Trade Commission. *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use?utm_source=govdelivery, (11 July 2022).
- United States of America, Federal Trade Commission. *Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security*, Commission File No. P065401, https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf, (1 October 2021).
- United States of America, Senate. *Data Accountability and Transparency Act 2020, Released as a Discussion Draft by Senator Sherrrod Brown*, <https://www.banking.senate.gov/imo/media/doc/DATA2020%20One-Pager.pdf>.
- United States of America, Senate, Letter of 13 April 2021, https://www.wyden.senate.gov/imo/media/doc/HainesBurns_WydenHeinrich_13APR21%20-FINAL.pdf, (13 April 2021).
- United States of America, Senate. *Protecting Americans' Data from Foreign Surveillance Act*, <https://www.wyden.senate.gov/imo/media/doc/Protecting%20Americans%20Data%20from%20Foreign%20Surveillance%20Act%20of%202021%20Bill%20Text.pdf>
- United States of America, Senate. *Safe Data Act*, <https://www.commerce.senate.gov/services/files/BD190421-F67C-4E37-A25E-5D522B1053C7>.
- United States of America, US Federal Register. *Executive Order 12333*, 46 FR 59941, 3 CFR, 1981 Comp., p. 200 (4 December 1981). (“EO 12333”).
- United States of America. *American Data Privacy and Protection Act*, H.R. 8152 (117th), (21 July 2022). (“ADPPA”).
- United States of America. Attorney General Order No. 3824-2017, *Judicial Redress Act of 2015*, 82 Fed. Reg. 7860, (23 January 2017).
- United States of America. *Children's Online Privacy Protection Rule*, 15 U.S.C. 6501-6508, (7 January 2013). (“COPPA”).
- United States of America. *CLOUD Act*, H.R.4943, (2018). (“Cloud Act”).
- United States of America. *Consumer Online Privacy Rights Act*, 116th Congress (2019-2020), S.2968. (“COPRA”).
- United States of America. *Data Care Act of 2021*, 117th Congress (2021-2022), S.919.
- United States of America. *Data Protection Act of 2020*, 116th Congress (2019-2020), S.3300.
- United States of America. *Deceptive Experiences To Online Users Reduction Act*, 116th Congress, S.1084.
- United States of America. *Electronic Communications Privacy Act of 1986*, 18 U.S.C. §§ 2510–2523. (“ECPA”).
- United States of America. Federal Trade Commission Act, 15 U.S.C. §§ 41-58. (“FTCA”).
- United States of America. *Filter Bubble Transparency Act*, 116th Congress, S.2763.
- United States of America. *FISA Amendments Reauthorization Act of 2017*, S.139, (19 January 2018).
- United States of America. *Foreign Intelligence Surveillance Act*, 50 U.S.C. Paras. 1801–11, 1821–29, 1841–46, 1861–62, 1871, (1978). (“FISA”).
- United States of America. *Health Insurance Portability and Accountability Act of 1996*, 104th United States Congress, Public Law 104-191. (“HIPPA”).
- United States of America. *Internal Revenue Service Rule*, 26 U.S.C. § 7216, (1986).

- United States of America. *International Communications Privacy Act*, 115th Congress (2017-2018), S.1671.
- United States of America. *Judicial Redress Act of 2015*, H.R. 1428 (114th), (24 February 2016). (“JRA”).
- United States of America. Office of the US Trade Representative. *Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text*, <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>, (1 July 2020).
- United States of America. *Online Privacy Act of 2019*, 116th Congress (2019-2020), H.R. 4978. (“OPA”).
- United States of America. *Public Law 114 - 23 - Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, H.R. 2048. (“Freedom Act”).
- United States of America. *Stored Communications Act*, 18 U.S.C. Chapter 121, Paras. 2701–2713, (1986). (“SCA”).
- United States of America. *The Constitution of the United States*, (4 March 1789).
- United States of America. *The LEADS Act*, S.512, H.R. 1174.
- United States of America. *The Privacy Act of 1974*, Public Law No. 93-579, 5 U.S.C. § 552 a. (“Privacy Act”).
- United States of America. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, H.R. 3162, Publ. L. No. 107–56, 115 Stat. 272, (26 October 2001). (“Patriot Act”).
- United States of America, Department of Defense. *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)*, <https://www.federalregister.gov/documents/2016/10/21/2016-25315/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for>, (16 October 2016).
- United States of America, National Institute of Standards and Technology. *Framework for Cyber-Physical Systems: Volume 1, Overview*, <https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview>, (26 June 2017).
- United States of America, Office of the United States Trade Representative. *Anti-Counterfeiting Trade Agreement (ACTA)*, <https://ustr.gov/acta>, (1 October 2011).
- United States of America, Senate Committee on Commerce, Science, and Transportation. (2022). *American Data Privacy and Protection Act Draft Legislation. Section by Section Summary*, <https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50>.
- United States of America, Senate Committee on Commerce, Science, and Transportation. *American Data Privacy and Protection Act Draft Legislation. Section by Section Summary*, <https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50>, (2022).
- United States of America, The White House. *Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies*, Executive Order 13959 of 12 November 2020, <https://www.federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies>, (17 November 2020).
- United States of America, The White House. *Big Data: Seizing opportunities, preserving values*, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, (May 2014).
- United States of America, The White House. *Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*, <https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence>, (7 October 2022). (“EO 14086”).
- United States of America, The White House. *Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States*, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states>, (15 September 2022).
- United States of America, The White House. *Fact Sheet: President Biden to Sign Executive Order Protecting Access to Reproductive Health Care Services*, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services>, (8 July 2022).
- United States of America, The White House. *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework>, (25 March 2022).
- United States of America, The White House. *Federal Big Data Research and Development Strategic Plan*, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/NSTC/bigdatardstrategicplan-nitrd_final-051916.pdf, (May 2016).
- United States of America, The White House. *Liberty and Security in a changing world*, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, (12 December 2013).
- United States of America, The White House. *Presidential Policy Directive -- Signals Intelligence Activities*, <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>, (17 January 2014). (“PPD-28”).
- United States of America, The White House. *The 2015 National Security Strategy*, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf, (6 February 2015).

- Unites States of America, *Trade Representative. 2019 National Trade Estimate Report on Foreign Trade Barriers*, https://ustr.gov/sites/default/files/2019_National_Trade_Estimate_Report.pdf, (15 March 2019).
- Unites States of America. *FISA Amendments Act of 2008*, H.R. 6304, (10 July 2008).
- Unites States of America. *FISA Amendments Act Reauthorization Act of 2012*, H.R. 5949, (30 December 2012).
- Unites States of America. *Fourth amendment of the US constitution, US congress*, <https://www.archives.gov/founding-docs/bill-of-rights-transcript#toc-amendment-iv>, (15 December 1791).
- Unites States of America. *PROTECT IP Act of 2011*, S.968 (112th), (26 May 2011).
- Unites States of America. *Stop Online Piracy Act*, H.R. 3261 (112th), (26 October 2011).
- The National People's Congress of the People's Republic of China. *Civil Code of the People's Republic of China*, <http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf>, (28 May 2020). ("Civil Code").
- The National People's Congress of the People's Republic of China. *Constitution of the People's Republic of China*, http://www.npc.gov.cn/zgrdw/englishnpc/Constitution/2007-11/15/content_1372964.htm, (4 December 1982).
- The National People's Congress of the People's Republic of China. *Cybersecurity Law of the People's Republic of China*, [hhttps://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china](https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china), (7 November 2016). ("CSL").
- The National People's Congress of the People's Republic of China. *Data Security Law of the People's Republic of China*, <http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>, (10 June 2021). ("DSL").
- The National People's Congress of the People's Republic of China. *Personal Information Protection Law of the People's Republic of China*, Chairman's Order No. 91, (20 August 2021). ("PIPL").
- World Trade Organization. *Agreement on Trade-Related Aspects of Intellectual Property Rights*, https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm, (15 April 1994).
- World Trade Organization. *Communication from the European Communities and their Member States. Coverage of CPC 84 – Computer and Related Services*, TN/S/W/6S/CSC/W/35, (24 October 2002).
- World Trade Organization. *Communication from the European Union, Joint statement on electronic commerce, EU proposal for WTO disciplines and commitments relating to electronic commerce*, INF/ECOM/22, https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf, (26 April 2019).
- World Trade Organization. *Declaration on Global Electronic Commerce*, WT/MIN(98)/DEC/2, (25 May 1998).
- World Trade Organization. *Electronic Commerce Negotiations, Consolidated Negotiating Text*, INF/ECOM/62/Rev.1, (14 December 2020).
- World Trade Organization. *General Agreement on Tariffs and Trade 1994*, https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm, (1994).
- World Trade Organization. *General Agreement on Trade in Services*, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm, (1995).
- World Trade Organization. *Joint statement on electronic commerce - Communication from Côte d'Ivoire*, INF/ECOM/4, (16 December 2019).
- World Trade Organization. *Joint Statement on Electronic Commerce. EU proposal for WTO disciplines and commitments relating to Electronic Commerce*, INF/ECOM/22, (26 April 2019).
- World Trade Organization. *Services sectoral classification list*, MTN.GNS/W/120, (10 July 1991).
- World Trade Organization. *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Panel*, WT/DS285/R, (10 November 2004).
- World Trade Organization. *Work Programme on Electronic Commerce - Communication from the United States*, S/C/W/359, (17 December 2014).

2. Decisions

- Council of the European Union. (10 December 2016). *Council Decision (EU) 2016/2220 of 2 December 2016 on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences*, OJ L 336, 1–2.
- Council of the European Union. (10 December 2019). *Council Decision (EU) 2019/2107 of 28 November 2019 on the position to be taken on behalf of the European Union within the Council of the International Civil Aviation Organization as regards the revision of Chapter 9 of Annex 9 (Facilitation) to the Convention on International Civil Aviation in respect of standards and recommended practices on passenger name record data*, OJ L 318, 117–122
- Council of the European Union. (19 May 2021). *Conclusions on the transfer of PNR data to third countries, in particular Australia and the United States*, ST 8635/21.
- Council of the European Union. (15 May 2009). *Council Decision of 6 April 2009 establishing the European Police Office (Europol)*, 2009/371/JHA, OJ L 121, 37–66.
- Council of the European Union. (2 December 2019). *Council conclusions on Europol's cooperation with Private Parties*, 14745/19, ENFOPOL 526.

- Council of the European Union. (20 June 2002). *Council Framework Decision of 13 June 2002 on joint investigation teams*, OJ L 162, 1–3.
- Council of the European Union. (24 August 2018). *Council Decision (EU) 2018/1197 of 26 June 2018 on the signing, on behalf of the European Union, and provisional application of the Strategic Partnership Agreement between the European Union and its Member States, of the one part, and Japan, of the other part*, ST/8461/2018/INIT, OJ L 216, 1–3.
- Council of the European Union. (29 December 2006). *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*, 2006/960/JHA, OJ L 386, 89–100.
- Council of the European Union. (30 December 2008). *Council framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, 2008/977/JHA, OJ L 350/60.
- Council of the European Union. (6 March 2002). *2002/187/JHA: Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime*, OJ L 63, 1–13.
- European Commission. (1 August 2016). *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, C/2016/4176, OJ L 207, 1–112.
- European Commission. (10 July 2023). *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final.
- European Commission. (15 June 2001). *Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC*, 2001/497/EC, OJ L 181, 19–31.
- European Commission. (16 December 2016). *Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council*, OJ L 344, C/2016/8471, 100–101.
- European Commission. (25 August 2000). *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*. 2000/520/EC. OJ L 215, 7–47.
- European Commission. (29 December 2004). *Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries*, OJ L 385, 2004/915/EC, 74–84.
- European Commission. (4 January 2002). *C2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)*, OJ L 2, 13–16.
- European Commission. (5 February 2010). *Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council*, OJ L 39, 2010/87, 5–18.
- European Data Protection Supervisor. (11 January 2022). *Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament*, https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf.

3. Judgments

- Court of Justice of the European Union. *Digital Rights Ireland v Commission*, case T-670/16, OJ C 410/26, ECLI:EU:T:2017:838, (7 November 2016).
- Court of Justice of the European Union. Judgment of the Court (First Chamber) of 3 October 2019, *Staatssecretaris van Justitie en Veiligheid v A and Others*. Case C 70/18. ECLI:EU:C:2019:823.
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 1 October 2015. *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*. C-230/14, ECLI:EU:C:2015:639. (“Weltimmo”).
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 10 February 2009, *Ireland v European Parliament and Council of the European Union*. Case C-301/06. ECLI:EU:C:2009:68.
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 13 May 2014. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. Case C-131/12. ECLI:EU:C:2014:317. (“Google Spain”).
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 16 July 2020. *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*. Case C-311/18. ECLI:EU:C:2020:559. (“Schrems II”).
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 21 June 2022, *Request for a preliminary ruling under Article 267 TFEU from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 17 October 2019, received at the Court on 31 October 2019, in the proceedings Ligue des droits humains v Conseil des ministres*, Case C-817/19, ECLI:EU:C:2022:497. (“Ligue des droits humains”).
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 24 September 2019. *Request for a preliminary ruling under Article 267 TFEU from the Conseil d'État (Council of State, France), made by decision of*

- 19 July 2017, received at the Court on 21 August 2017, in the proceedings *Google LLC, successor in law to Google Inc.* Case C-507/17. ECLI:EU:C:2019:772.
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 3 June 2008, *The Queen, on the application of International Association of Independent Tanker Owners (Intertanko) and Others v Secretary of State for Transport*, C-308/06, ECLI:EU:C:2008:312.
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 30 May 2006. *European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04)*. Cases C-317/04 and C-318/04. ECLI:EU:C:2006:346.
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd*, C 210/16, ECLI:EU:C:2018:388. ("Facebook fanpages").
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 6 October 2015. *Maximilian Schrems v Data Protection Commissioner*. Case C-362/14. ECLI:EU:C:2015:650. ("Schrems I").
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and others v Conseil des ministres*, ECLI:EU:C:2020:791.
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 6 October 2020. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Other*. Case C-623/17. ECLI:EU:C:2020:790.
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland v Seitlinger and Others*, C-293/12, ECLI:EU:C:2014:238.
- Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 8 March 2011, *Lesoochránárske zoskupenie VLK v Ministerstvo životného prostredia Slovenskej republiky*, Case C-240/09, ECLI:EU:C:2011:125.
- Court of Justice of the European Union. Judgment of the Court of 12 November 1969. *Erich Stauder v City of Ulm – Sozialamt*. Case 29-69. ECLI:EU:C:1969:57. European Court reports 1969, 419–426.
- Court of Justice of the European Union. Judgment of the Court of 14 May 1974. *J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities*. Case 4-73. ECLI:EU:C:1974:51.
- Court of Justice of the European Union. Judgment of the Court of 15 July 1964. *Flaminio Costa v E.N.E.L.* Case 6-64. ECLI:EU:C:1964:66. European Court reports 1964, 1251 ff.
- Court of Justice of the European Union. Judgment of the Court of 16 June 1998, *A. Racke GmbH & Co. v Hauptzollamt Mainz*, C-162/96, ECLI:EU:C:1998:293.
- Court of Justice of the European Union. Judgment of the Court of 17 December 1970. *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*. Case 11-70. ECLI:EU:C:1970:114.
- Court of Justice of the European Union. Judgment of the Court of 24 November 1992, *Anklagemyndigheden v Peter Michael Poulsen and Diva Navigation Corp*, C-286/90, ECLI:EU:C:1992:453.
- Court of Justice of the European Union. Judgment of the Court of 28 July 2016, *Verein für Konsumenteninformation v Amazon EU Sàrl*, C-191/15, ECLI:EU:C:2016:612. ("Verein für Konsumenteninformation").
- Court of Justice of the European Union. Judgment of the Court of 30 April 1974, *R. & V. Haegeman v Belgian State*, Case 181-73, ECLI:EU:C:1974:41.
- Court of Justice of the European Union. Judgment of the Court of 4 July 2023, Case C-252/21, ECLI:EU:C:2023:537.
- Court of Justice of the European Union. Judgment of the Court of 4 July 2023, *Meta Platforms and Others v Bundeskartellamt*, Case C-252/21, ECLI:EU:C:2023:537.
- Court of Justice of the European Union. Judgment of the Court of 8 April 2014, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.
- Court of Justice of the European Union. Judgment of the Court of 8 April 2014, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others*, joined cases C-293/12 and C-594/12, Opinion of the Advocate General Mengozzi delivered on 8 September 2016, ECLI:EU:C:2016:656.
- Court of Justice of the European Union. *Opinion 1/15 of the CJEU (Grand Chamber)*, ECLI:EU:C:2017:592.
- Court of Justice of the European Union. Opinion of Advocate General Saugmandsgaard Oe delivered on 19 December 2019. *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*. Case C-311/18. ECLI:EU:C:2019:1145.
- Court of Justice of the European Union. *Opinion of the Court (Full Court) of 18 December 2014*. Case Opinion 2/13. ECLI:EU:C:2014:2454.
- ECtHR, *Caroline von Hannover v Germany*, Applications no. 40660/08 and no. 60641/08, (7 February 2012).
- ECtHR, *Handyside v. UK*, Application no. 5493/72, (7 December 1976).
- European Court of Human Rights. Judgment of 1 October 2008, *Liberty and others v. The United Kingdom*, Application no. 58243/00.
- European Court of Human Rights. Judgment of 12 June 2003, *van Kück v. Germany*, Application no. 35968/97.
- European Court of Human Rights. Judgment of 13 November 2012, *M.M. v the United Kingdom*, Application no. 24029/07.
- European Court of Human Rights. Judgment of 17 February 2011, *Wasmuth v Germany*, Application no. 12884/03.

- European Court of Human Rights. Judgment of 18 August 2010, *Kennedy v. The United Kingdom*, Application no. 26839/05.
- European Court of Human Rights. Judgment of 19 September 2013, *von Hannover v Germany*, Application no. 8772/10.
- European Court of Human Rights. Judgment of 2 September 2010, *Uzun v Germany*, Application no. 35623/05.
- European Court of Human Rights. Judgment of 25 February 1997, *Z. v Finland*, Application no. 22009/93.
- European Court of Human Rights. Judgment of 26 March 1987, *Leander v Sweden*, Application no. 9248/81.
- European Court of Human Rights. Judgment of 28 January 2003, *Peck v United Kingdom*, Application no. 44647/98.
- European Court of Human Rights. Judgment of 4 December 2008, *S. u. Marper v UK*, Application no. 30562/04.
- European Court of Human Rights. Judgment of 4 May 2000, *Rotaru v. Romania*, Application 28341/95.
- European Court of Human Rights. Judgment of 6 September 1978, *Klass et al v. Germany*, Application no. 5029/71.
- European Court of Human Rights. Judgment of 7 July 2011, *Al-Skeini and others v. The United Kingdom*, Application no. 55721/07.
- German Federal Cartel Office (BKartA), Judgment of 6 February 2019, B6-22/16.
- German Federal Constitutional Court (BVerfG). BVerfGE 37, P. 271 ff. (“*Solange I*”).
- German Federal Constitutional Court (BVerfG). Judgment of the First Senate of 15 December 1983, 1 BvR 209/83 et al., Paras. 1–215.
- German Federal Constitutional Court (BVerfG). Judgment of the Second Senate of 13 October 2016, 2 BvR 1368/16, Paras. 1–73.
- International Court of Justice. *Nicaragua v. United States of America*, Judgment of 27 June 1986, (27 June 1986).
- International Court of Justice. *North Sea Continental Shelf Cases*, Judgment of 20 February 1969, Reports of judgments, advisory opinions and orders.
- International Court of Justice. *Nottebohm (Liechtenstein v. Guatemala)*, Summary of the Judgment of 6 April 1955, <https://www.icj-cij.org/public/files/case-related/18/2676.pdf>, (6 April 1955).
- International Court of Justice. *S.S. Lotus (France v. Turkey)*, 1927 P.C.I.J. (ser. A) No. 10, (7 September 1927).
- Italian Constitutional Court. Sent. 183/7.
- Kammergericht, Fliegender Gerichtsstand*, 5 W 371/07, 25 January 2008. P. 212.
- Oberster Gerichtshof der Republik Österreich, OGH 6 Ob 56/21k*, ECLI:AT:OGH0002:2021:E132244, (23 June 2021).
- United States of America. *American Civil Liberties Union v. James Clapper*, Court of Appeals for the Second Circuit, Case 14-42, (7 May 2015).
- United States of America. *Banken Trust Co.*, US Court of Appeals for the Sixth Circuit, 61 F.3d 465 [469], (3 August 1995).
- United States of America. *Carpenter v. United States*, Supreme Court, No. 16–402, (22 June 2018).
- United States of America. Court of Appeals for the Ninth Circuit, Case 13-50572, (2 September 2020).
- United States of America. District Court Southern District of New York, 13 Mag. 2814, (25 April 2014).
- United States of America. *Federal Bureau of Investigation et al v. Fazaga et al*, Supreme Court, No. 20-828, (4 March 2022).
- United States of America. *Hester v. United States*, Supreme Court, 265 U.S. 57, (1924).
- United States of America. *Hunter Douglas, Inc. v. Comfortex Corp.*, No. Civ. 98 Civ. 479.
- United States of America. *In re Search Warrant No. 16-960-M-01 to Google*, United States District Court, E.D. Pennsylvania, 232 F. Supp.3d 708, (3 February 2017).
- United States of America. *IND. FOUNDATION, ETC. v. Texas Ind. Acc. Bd.*, Supreme Court of Texas, 540 S.W.2d 668 (1976).
- United States of America. Judgment of 14 July 2016, Court of Appeals for the 2nd Circuit New York, Case No. 14–298, (14 July 2016).
- United States of America. *Katz v. United States*, Supreme Court, 389 U.S. 347, (1967).
- United States of America. *Kelley v. Euromarkiet Designs, Inc.*, United States District Court, E.D. California, No. Civ S-07-2302, (7 January 2008).
- United States of America. *Linde v. Arab Bank, PLC*, United States District Court, E.D. New York, 262 F.R.D., 136 [139], (22 May 2009).
- United States of America. *Microsoft Corporation v. United States of America*, 2d Cir., Case No. 14-2985, (14 July 2016).
- United States of America. *Morgan Art Foundation Ltd. v. McKenzie, American Image Art et al*, District Court of Southern District of New York, 18 Civ. 4438 (AT), (15 December 2021).
- United States of America. *Morrison v. National Australia Bank*, Supreme Court, 561 U.S. 247, (24 June 2010).

- United States of America. *Obama v. Klayman*, Court of Appeals, D. C. Circuit, Case 14-5004, (28 August 2015).
- United States of America. *Planned Parenthood of South-eastern Pennsylvania et al. v. Casey*, Supreme Court, 505 U.S. 833, (1992).
- United States of America. *Richmark Corp. v. Timber Falling*, 959 F. 2d 146, 9th Cir., (1992).
- United States of America. *Roe v. Wade*, Supreme Court, No. 70-18, (1973).
- United States of America. *Seal v. Jefferson B. Sessions III*, Court of Appeals Ninth Circuit, Cases No. 16-16067, 16-16081, and 16-16082, (17 July 2017).
- United States of America. *Smith v. Maryland*, Supreme Court, 442 U.S. 735, (1979).
- United States of America. *Société Nationale Aérospatiale v. US District Court*, 482 U.S. 522, (1987)
- United States of America. *Thomas E. Dobbs, State Health Officer of the Mississippi Department of Health, et al., Petitioners v. Jackson Women's Health Organization, et al.*, Supreme Court, No. 19-1392, (2022).
- United States of America. *Transunion LLC v. Ramirez*, Supreme Court, No. 20-297.
- United States of America. *United States Department of Justice v. Reporters Committee For Freedom of the Press*, 489 U.S. 749, (1989).
- United States of America. *United States v. Miller*, Supreme Court, 425 U.S. 435, (1976).
- United States of America. *US Agency for Int'l Dev. v. Alliance for Open Soc'y Int'l, Inc.*, Supreme Court, 140 S. Ct. 2082, 2086 (2020)
- United States of America. *Whalen v. Roe*, Supreme Court, 429 U.S. 589, (1977).
- United States of America. *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme*, Court of Appeals for the Ninth Circuit, 145 F. Supp.2d 1168, 1180 (N.D. Cal. 2001).
- United States of America. *Youngstown Sheet & Tube Co. v. Sawyer*, Supreme Court, 343 U.S. 579 (1952).
- Verwaltungsgericht Wiesbaden. Judgment of 20 November 2021, Az. 6 L 738/21.WI, (1 December 2021).

4. Books

- Allen, A. [Anita]. (1988). *Uneasy access*. Rowman & Littlefield.
- Bachmann, G. [Gregor]. (2006). *Private Ordnung*. Mohr Siebeck.
- Bennett, C. [Colin] and Raab, C. [Charles]. (2006). *The Governance of Privacy*. The MIT Press.
- Bok, S. [Sissela]. (1982). *Secrets: On the Ethics of Concealment and Revelation*. Pantheon Books.
- Borking, J. [John]. (1998). *Privacy-enhancing Technologies: The Path to Anonymity*. Registratiekamer.
- Cate, F. [Fred]. (1997). *Privacy in the information age*. Brookings Institution Press.
- Constantinesco, L.-J. [Léontin-Jean]. (1972). *Die rechtsvergleichende Methode*. Vol. 2. Heymanns.
- Dutta, S. [Soumitra] and Mia, I. [Irene]. (2010). *Global Information Technology Report 2009-2010*. World Economic Forum.
- Ehmann, E. [Eugen] and Selmayr, M. [Martin]. (2018). *Datenschutz-Grundverordnung: DS-GVO*. C.H. Beck.
- Fischer-Lescano, A. [Andreas] and Teubner, G. [Gunther]. (2006). *Regime-Kollisionen: Zur Fragmentierung des globalen Rechts*. Suhrkamp.
- Fischer-Lescano, A. [Andreas]. (2005). *Globalverfassung: Die Geltungsbegründung der Menschenrechte*. Velbrück.
- Greenleaf, G. [Graham]. (2017). *Asian Data Privacy Laws*. Oxford University Press.
- Greenwald, G. [Glen]. (2015). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Picador USA.
- Gunningham, N. [Neil] and Grabosky, P. [Peter]. (1998). *Smart Regulation: Designing Environmental Policy*. Clarendon Press.
- Herdegen, M. [Matthias]. (2019). *Der Kampf um die Weltordnung*. C.H. Beck.
- Herdegen, M. [Matthias]. (2020). *Internationales Wirtschaftsrecht*. C.H. Beck.
- Hildebrandt, M. [Mireille]. (2020). *Law for Computer Scientists and Other Folk*. Oxford University Press.
- Hilf, M. [Meinhard] and Oeter, S. [Stefan]. (2010). *WTO-Recht, Rechtsordnung des Welthandels*. Nomos.
- Hoeren, T. [Thomas]. (1995). *Selbstregulierung im Banken- und Versicherungsrecht*. Verlag Versicherungswirtschaft.
- Holdgaard, R. [Rass]. (2008). *External Relations Law of the European Community*. Wolters Kluwer.
- Jessup, P. [Philip]. (1956). *Transnational Law*. Yale University Press.
- Kant, I. [Immanuel]. (1796). *Zum ewigen Frieden. Ein philosophischer Entwurf. Neue vermehrte Auflage*. Frankfurt und Leipzig.

- Kischel, U. [Uwe]. (2019). *Comparative law*. Oxford University Press.
- Kropholler, J. [Jan]. (1975). *Internationales Einheitsrecht*. Mohr Siebeck.
- Kuner, C. [Christopher] and Bygrave, L. A. [Lee A.] and Docksey, C. [Christopher] and Drechsler, L. [Laura] (eds.). (2020). *The EU General Data Protection Regulation (GDPR), A Commentary*. Oxford University Press.
- Kuner, C. [Christopher]. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.
- McCarthy, J. T. [J. Thomas]. (1994). *The Rights of Publicity and Privacy*. Clark Boardman Callaghan.
- McCarthy, T. [Thomas]. (1999). *The rights of publicity and privacy*. Clark Boardman Callaghan.
- Miller, A. [Arthur]. (1971). *Der Einbruch in die Privatsphäre*. Luchterhand.
- Moerel, L. [Lokke]. (2012). *Binding Corporate Rules*. Oxford University Press.
- Naef, T. [Tobias]. (2023). *Data Protection without Data Protectionism*. Springer.
- Newman, A. L. [Abraham L.]. (2008). *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Cornell University Press.
- Noll, P. [Peter]. (1973). *Gesetzgebungslehre*. Rowohlt.
- Nowak, M. [Manfred]. (2005). *UN Covenant on Civil and Political Rights. CCPR Commentary*. Engel.
- Perry, S. [Susan] and Roda, C. [Claudia]. (2017). *Human Rights and Digital Technology*. Palgrave Macmillan.
- Polcak, R. [Radim] and Svantesson, D. J. B. [Dan Jerker B.]. (2017). *Information Sovereignty. Data Privacy, Sovereign Powers and the Rule of Law*. Edward Elgar.
- Raab C. [Charles] et al. (1999). *Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: Test of the method on several categories of transfer*. Office for Official Publications of the European Communities.
- Röhl, K. [Klaus]. (2006). *Rechtssoziologie: Ein Lehrbuch*. Carl Heymanns.
- Roßnagel, A. [Alexander] and Geminn, C. [Christian]. (2020). *Datenschutz-Grundverordnung verbessern*. Nomos.
- Schiff Berman, P. [Paul]. (2012). *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders*. Cambridge University Press.
- Schwartz, P. [Paul] and Solove, D. [Daniel]. (2021). *Information Privacy Law*. Wolters Kluwer.
- Solove, D. [Daniel]. (2008). *Understanding Privacy*. Harvard University Press.
- Svantesson, D. J. B. [Dan Jerker B.]. (2013). *Extraterritoriality in Data Privacy Law*. Ex Tuto Publishing.
- United Nations Conference on Trade and Development. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>.
- United Nations. (2013). *Yearbook of the International Law Commission 2006. A/CN.4/SER.A/2006/Add.1 (Part 2)*. United Nations publications.
- Viellechner, L. [Lars]. (2013). *Transnationalisierung des Rechts*. Velbrück.
- Wielsch, Dan. (2008). *Zugangsregeln: die Rechtsverfassung der Wissensteilung*. Mohr Siebeck.
- Zimmermann, S. [Stefan]. (2009). *E-Commerce, Verbraucherschutz und die Entwicklung Intelligenter Agenten*. Peter Lang.

5. E-books

- Altmaier, P. [Peter] et al. (2019). *Project GAIA-X*. Federal Ministry for Economic Affairs and Energy. https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=5.
- Blumtritt, C. [Christoph] et al. (2021). *Digital Economy Compass 2021*. Statista GmbH. <https://de.statista.com/statistik/studie/id/105648/dokument/digital-economy-compass>.
- Buss, S. [Sebastian] et al. (2019). *Digital Economy Compass 2019*. Statista GmbH. <https://de.statista.com/statistik/studie/id/52312/dokument/digital-economy-compass>.
- Casalini, F. [Francesca]; López González, J. [Javier]. (2019). *Trade and cross-border data flows*. OECD Publishing. <https://doi.org/10.1787/b2023a47-en>.
- Chase P. [Peter] et al. (July 2016). *Transatlantic digital economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU%282016%29535006_EN.pdf.
- D' Acquistio, G. [Giuseppe] et al. (2015). *Privacy by design in big data*. ENISA. https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport.
- De Bièvre, M. [Matthias] et al. (2020). *35 proposals to make the European data strategy work*. Sitra. <https://www.sitra.fi/en/publications/35-proposals-to-make-the-european-data-strategy-work>.
- Fischer, P. E. [Philipp Eberhard]. (2012). *Will Privacy Law in the 21st Century be American, European or International?*. GRIN Verlag. <https://www.grin.com/document/187981>.

- Madiega, T. [Tambiama]. (2020). *Reform of the EU liability regime for online intermediaries, Background on the forthcoming digital services act*. European Parliamentary Research Service.
- Ministry of Industry and Trade of Vietnam. (2020). *Regulations, Policies and Initiatives on E-Commerce and digital economy for APEC MSMEs' Participation in the Region*. Asia-Pacific Economic Cooperation Secretariat. https://www.apec.org/docs/default-source/publications/2020/3/regulations-policies-and-initiatives-on-e-commerce-and-digital-economy/220ecsgregulations-policies-and-initiatives-on-ecommerce-and-digital-economy-for-apec-msmes-particip.pdf?sfvrsn=63b748d7_1.
- Organisation for Economic Co-operation and Development. (2015). *OECD Digital Economy Outlook 2015*. OECD Publishing. <https://doi.org/10.1787/9789264232440-en>.
- Organisation for Economic Co-operation and Development. (24 July 2006). *Making Privacy Notices Simple: An OECD Report and Recommendations, OECD digital economy Papers, No. 120*. OECD Publishing. <https://doi.org/10.1787/231428216052>.
- Reinsel, D. [David]. (2017). *Data Age 2025: The Evolution of Data to Life-Critical*. IDC White Paper. <https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>.
- United Nations Conference on Trade and Development. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow*. United Nations Publications. <https://doi.org/10.18356/9789210058254>.
- von der Leyen, U. [Ursula]. (2019). *Union that strives for more. My agenda for Europe*. Publications Office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1>.

6. Thesis

- Iakovleva, S. [Svetlana]. (2021). *Governing cross-border data flows: Reconciling EU data protection and international trade law*. [Doctoral thesis, Faculty of Law, Universiteit van Amsterdam (I. Venzke)]. <https://hdl.handle.net/11245.1/cf54d2a9-cd41-42c2-94f1-24c81f8a3abd>.

7. Chapters or parts of a book

- Atkinson, R. [Robert] and Cory, N. [Nigel]. (2021). Cross-Border Data Policy: Opportunities and Challenges. In H. [Huiyao] Wang and A. [Alistair] Michie, *Consensus or Conflict? China and Globalization in the 21st Century* (pp. 217–232). Springer.
- Birger, A. [Arndt]. (2012). Das Risikoverständnis der Europäischen Union unter besonderer Berücksichtigung des Vorsorgeprinzips. In L. [Liv] Jaeckel and G. [Gerold] Janssen, *Risikodogmatik im Umwelt- und Technikrecht* (pp. 35–50). Mohr Siebeck.
- Buttarelli, G. [Giovanni]. (2020). Foreword. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. v–vi). Oxford University Press.
- Bygrave, L. A. [Lee A.] (2008). International agreements to protect personal data. In J. [James] Rule and G. [Graham] Greenleaf, *Global privacy protection* (pp. 15–49). Edward Elgar.
- Chirwa, D. [Danwood]. (2019). State Responsibility for Human Rights. In M. [Manisuli] Ssenyonjo, *International Human Rights Law. Six Decades after the UDHR and Beyond* (pp. 397–410). Routledge.
- de Terwangne, C. [Cécile]. (2009). Is a Global Data Protection Regulatory Model Possible? In S. [Serge] Gutwirth and Y. [Yves] Pouillet and P. [Paul] De Hert and C. [Cécile] de Terwangne and S. [Sjaak] Nouwt (eds.), *Reinventing Data Protection?* (pp. 175–189). Springer.
- Drexl, J. [Josef]. (2016). Regulierung der Cyberwelt – Aus dem Blickwinkel des internationalen Wirtschaftsrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 95–158). C.F. Müller Verlag.
- Drexl, J. [Josef]. (2019). Digital economy and the disruption of traditional concepts. In A. [Alberto] De Franceschi and R. [Reiner] Schulze, *Digital Revolution - New Challenges for Law* (pp. 19–40). Nomos.
- Farrell, H. [Henry]. (2012). Negotiating Privacy across Arenas - The EU-US 'Safe Harbor' Discussions. In A. [Adrienne] Windhoff-Héritier, *Common Goods: Reinventing European Integration Governance* (pp. 101–123). Rowman & Littlefield.
- Fernandes, M. [Mário] and Rodrigues da Silva, A. [Alberto]. (2018). Specification of Personal Data Protection Requirements: Analysis of Legal Requirements based on the GDPR Regulation. In *Proceedings of the 20th International Conference on Enterprise Information Systems - Volume 2, ICEIS*, (pp. 398–405). SciTePress.
- Goldfarb, A. [Avi] and Trefler, D. [Daniel]. (2019). Artificial intelligence and international trade. In A. [Ajay] Agrawal and J. [Joshua] Gans and A. [Avi] Goldfarb (eds.), *The Economics of Artificial Intelligence* (pp. 463–492). University of Chicago Press.
- Greenleaf, G. [Graham]. (2014). A world data privacy treaty? 'Globalisation' and 'modernisation' of Council of Europe Convention 108. In N. [Normann] Witzleb and D. [David] Lindsay and M. [Moira] Paterson and S. [Sharon] Rodrick, *Emerging Challenges in Privacy Law* (pp. 92-138). Cambridge University Press.
- Ibáñez, J. [Josep]. (2008). Who Governs the Internet? The Emerging Regime of E-Commerce. In A. [Andreas] Nölke and J.-C. [Jean-Christophe] Graz, *Transnational Private Governance and its Limits* (pp. 142–155). Routledge.

- Kuner, C. [Christopher]. (2009). Developing an Adequate Legal Framework for International Data Transfers. In S. [Serge] Gutwirth and Y. [Yves] Poulet and P. [Paul] de Hert and C. [Cécile] and S. [Sjaak] Nouwt (ed.), *Reinventing Data Protection?* (pp. 263–275). Springer.
- Kuner, C. [Christopher]. (2020). Art. 44. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 755–770). Oxford University Press.
- Kuner, C. [Christopher]. (2020). Art. 48. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 825–840). Oxford University Press.
- Lange and Filip. (2020). DS-GVO Art. 49 Ausnahmen für bestimmte Fälle. In S. [Stefan] Brink and H. A. [Heinrich Amadeus] Wolff, *BeckOK Datenschutzrecht*. C.H. Beck. https://beck-online.beck.de/Bcid/Y-400-W-BECKOKDATENS-G-EWG_DSGVO-A-49-GI-A-II-1.
- Lynskey, O. [Orla]. (2021). Extraterritorial Impact Through an EU Law Lens. In F. [Federico] Fabbrini and E. [Eduardo] Celeste and J. [John] Quinn, *Data Protection Beyond Borders*, (pp. 191–209).
- Reiman, J. [Jeffrey]. (1984). Privacy, intimacy, and personhood. In F. D. [Ferdinand David] Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (pp. 300–316). Cambridge University Press
- Röben, V. [Volker]. (1999). International Internet Governance. In J. [Jost] Delbrück and R. [Rainer] Hofmann, *German Yearbook of International Law - Jahrbuch für Internationales Recht.: Vol. 42 (1999)* (pp. 400–437). Duncker & Humblot.
- Sand, I.-J. [Inger-Johanne]. (2009). Hybrid Law: Law in a Global Society of Differentiation and Change. In G.-P. [Graf-Peter] Calliess and A. [Andreas] Fischer-Lescano and D. [Dan] Wielsch and P. [Peer] Zumbansen, *Soziologische Jurisprudenz: Festschrift für Gunther Teubner zum 65. Geburtstag* (pp. 871–886). De Gruyter.
- Steinrötter, B. [Björn]. (2020). Legal Framework for Commercialisation of Digital Data. In M. [Martin] Ebers and S. [Susana] Navas (eds.), *Algorithms and Law* (pp. 269–298). Cambridge University Press.
- Svantesson, D. J. B. [Dan Jerker B.]. (2020). Art. 3. In C. [Christopher] Kuner and L. [Lee] Bygrave and C. [Christopher] Docksey and L. [Laura] Drechsler (eds.), *The EU General Data Protection Regulation (GDPR), A Commentary* (pp. 74–99). Oxford University Press.
- Von Arnould, A. [Andreas]. (2016). Freiheit und Regulierung in der Cyberwelt: Transnationaler Schutz der Privatsphäre aus Sicht des Völkerrechts. In N. [Nina] Dethloff and G. [Georg] Nolte and A. [August] Reinisch (eds.), *Freiheit und Regulierung in der Cyberwelt - Rechtsidentifikation zwischen Quelle und Gericht* (pp. 1–34). C.F. Müller Verlag.
- Witzleb, N. [Normann] and Lindsay, D. [David] and Paterson, M. [Moira] and Rodrick, S. [Sharon]. (2014). An overview of emerging challenges in privacy law. In N. [Normann] Witzleb and D. [David] Lindsay and M. [Moira] Paterson and S. [Sharon] Rodrick, *Emerging Challenges in Privacy Law* (pp. 1–28). Cambridge University Press

8. Articles

- Abbott, K. W. [Kenneth Wayne] and Snidal, D. [Duncan]. (2000). Hard and Soft Law in International Governance. *International Organization*, 54(3), 421–456.
- Amstutz, M. [Marc]. (2005). In-Between Worlds: Marleasing and the Emergence of Interlegality in Legal Reasoning. *European Law Journal*, 11(6), 766–784.
- Ash, K. [Kristina]. (2005). U.S. Reservations to the International Covenant on Civil and Political Rights: Credibility Maximization and Global Influence. *Northwestern Journal of International Human Rights*, 3(1), Article 7.
- Baisch, R. [Rainer] and Weber, R. [Rolf]. (2018). Revisiting the Public Moral/Order and the Security Exceptions under the GATS. *Asian Journal of WTO & International Health Law and Policy*, 13(2), 375–394.
- Barelli, M. [Mauro]. (2009). The Role of Soft Law in the International Legal System: The Case of the United Nations Declaration on the Rights of Indigenous Peoples. *International & Comparative Law Quarterly*, 58(4), 957–983.
- Bäumer, U. [Ulrich] and Mara, P. [Prashant] and Meeker, H. [Heather]. (2012). IT outsourcing and offshoring. *Computer Law Review International*, 13(1), 9–19.
- Bloustein, E. [Edward]. (1964). *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*. *New York University Law Review*, 39(6), 962–1007.
- Blume, P. [Peter]. (2011). Data Protection in the Cloud. *Computer Law Review International*, 12(3), 76–80.
- Boullenois, C. [Camille]. (2021). China's Data Strategy. *European Union Institute for Security Studies*, Brief 21.
- Bradford, A. [Anu]. (2012). The Brussels Effect. *Northwestern University Law Review*, 107(1), Columbia Law and Economics Working Paper No. 533, <https://ssrn.com/abstract=2770634>.
- Brandeis, L. [Louis] and Warren, S. [Samuel]. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220.
- Buchner, B. [Benedikt]. (2019). Datenschutz und Kartellrecht. *Wettbewerb in Recht und Praxis 2019*, 1243–1248.
- Burchard, C. [Christoph]. (2019). Europäische E-Evidence-Verordnung. *Zeitschrift für Rechtspolitik*, 2019(6), 164–167.
- Bygrave, L. A. [Lee A.]. (2000). European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation. *Computer Law & Security Review*, 16(4), 252–257.
- Calliess, C. [Christian]. (2002). Inhalt, Dogmatik und Grenzen der Selbstregulierung im Medienrecht. *AfP 2002*(6), 465–475.
- Carvalho, G. [Graca] and Kazim, E. [Emre]. (2022). Themes in data strategy: thematic analysis of 'A European Strategy for Data' (EC). *AI and Ethics*, 2(2), 53–63.

- Cohn, M. [Margit]. (2015). Non-Statutory Executive Powers in Five Regimes: Assessing Global Constitutionalism in Structural-Institutional Contexts. *The International and Comparative Law Quarterly*, Cambridge University Press, 64(1), 65–102.
- Colonna, L. [Liane]. (2014). Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?. *International Data Privacy Law*, 4(3), 203–221.
- Cunningham, M. [McKay]. (2013). Diminishing Sovereignty: How European Privacy Law Became International Norm. *Santa Clara Journal of International Law*, 11(2), 421–453.
- Denza, E. [Eileen]. (2008). A note on Intertanko, *European Law Review* 33, 870-879.
- Dupuy, P.-M. [Pierre-Marie]. (1991). Soft Law and the International Law of the Environment. *Michigan Journal of International Law*, 12(2), 420–435.
- Engel, C. [Christoph]. (2000). Das Internet und der Nationalstaat. Völkerrecht und Internationales Privatrecht in einem sich globalisierenden internationalen System – Auswirkungen der Entstaatlichung transnationaler Rechtsbeziehungen. *Berichte der Deutschen Gesellschaft für Völkerrecht*, 39, 353–425.
- Flemming, M. [Moos] and Rothkegel, T. [Tobias]. (2020). EU-US-Datenschutzschild ungültig – Schrems II. *Zeitschrift für Datenschutz*, 2020(10), 511–527.
- Fried, C. [Charles]. (1968). Privacy. *Yale Law Journal*, 77(3), 475–493.
- Funke, M. [Michael] and Wittmann, J. [Jörn]. (2013). Cloud Computing – ein klassischer Fall der Auftragsdatenverarbeitung? Anforderungen an die verantwortliche Stelle. *Zeitschrift für Datenschutz*, 2013(5), 221–228.
- Gasser, U. [Urs]. (2015). Perspectives on the Future of Digital Privacy. *Zeitschrift für Schweizerisches Recht*, 2015(2), 339–448.
- Gellert, R. [Raphaël]. (2015). Data protection: a risk regulation? Between the risk regulation of everything and the precautionary alternative. *International Data Privacy Law*, 5(1), 3–19. Oxford University Press.
- Grabenwarter, C. [Christoph]. (2010). Wirkungen eines Urteils des Europäischen Gerichtshofs für Menschenrechte – am Beispiel des Falls M. gegen Deutschland, *Juristenzeitung* 65(18), 857–869.
- Greenleaf, G. [Graham] and Cottier, B. [Bertil]. (2020). 2020 Ends a Decade of 62 New Data Privacy Laws. *Privacy Laws & Business International Report*, Vol. 163, 24–26.
- Greenleaf, G. [Graham]. (2005). The APEC Privacy Framework - A new low standard. *Privacy Laws & Business International Reporter*, 11(5). <http://classic.austlii.edu.au/au/journals/PrivLawPRpr/2005/1.html>.
- Greenleaf, G. [Graham]. (2009). Five Years of the Apec Privacy Framework: Failure or Promise?. *Computer Law & Security Report*, 25(1), 28–43.
- Greenleaf, G. [Graham]. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, 2(2), 68–92.
- Greenleaf, G. [Graham]. (2021). China's Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report*, 2021(172), <https://ssrn.com/abstract=3989775>.
- Heidenstecker, K. [Karin]. (1979). Zur Rechtsverbindlichkeit von Willensakten der Generalversammlung. *Zeitschrift für die Vereinten Nationen und ihre Sonderorganisationen*, 1979(6), 205–210.
- Hunt, J. [Jo]. (2010). Devolution and differentiation: Regional variation in EU law. *Legal Studies*, 30(3), 421–441.
- Hustinx, P. [Peter]. (2010). Privacy by design: delivering the promises. *Identity in the Information Society*, 3(2), 253–255.
- Ismail, N. [Noriswadi]. (2011). Cursing the Cloud (or) Controlling the Cloud?. *Computer Law & Security Review*, 27(3), 250–257.
- Janeček, V. [Václav]. (2018). Ownership of Personal Data in the Internet of Things. *Computer Law & Security Review*, 34(5), 1039–1052.
- Jarvis Thomson, J. [Judith]. (1975). The Right to Privacy. *Philosophy & Public Affairs*, 4(4), 295–314- P 295.
- Johnson, D. R. [David Reynold] and Post, D. [David G.]. (1996). Law and Borders - the Rise of Law in Cyberspace. *Stanford Law Review*, 48(5), 1367–1402.
- Jourard, S. [Sidney]. (1966). Some Psychological Aspects of Privacy. *Law and Contemporary Problems*, 31(2), 307–318.
- Kamba, W. [Walter]. (1974). Comparative Law: A Theoretical Framework. *International and Comparative Law Quarterly*, 23(3), 485–519.
- Keller, A. [Anja]. (2019). Tagungsbericht: PinG-Jahrestagung Datenschutz. *Kommunikation & Recht*, 2019(4), P. IX.
- Kennedy, G. [Gabriela] and Doyle, S. [Sara] and Lui, B. [Brenda]. (2009). Data protection in the Asia-Pacific region. *Computer Law & Security Review*, 25(1), 59–68.
- Kobrin, S. [Stephen]. (2004). Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 30(1), 111–131.
- Kokott, J. [Juliane] and Sobotta, C. [Christoph]. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), 222–228.
- Konstadinides, T. [Theodore]. (2012). When in Europe: Customary International Law and EU Competence in the Sphere of External Action. *German Law Journal*, 13(11), 1177–1202.
- Kötz, H. [Hein]. (1986). Rechtsvereinheitlichung – Nutzen, Kosten, Methoden, Ziele. *Rebels Zeitschrift für ausländisches und internationales Privatrecht*, 50(1), 1–18.

- Kuner, C. [Christopher]. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, 25(4), 307–317.
- Kuner, C. [Christopher]. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 1). *International Journal of Law and Information Technology*, 18(2), 176–193.
- Kuner, C. [Christopher]. (2015). Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. *International Data Privacy Law*, 5(4), 235–245.
- Ladeur, K.-H. [Karl-Heinz]. (2011). Ein Recht der Netzwerke für die Weltgesellschaft oder Konstitutionalisierung der Völkergemeinschaft?. *Archiv des Völkerrechts*, 49(3), 246–275.
- Lando, O. [Ole]. (1992). Principles of European Contract Law - An Alternative or a Precursor of European Legislation. *RabelsZ*, Vol. 56 (1992), 261 ff.
- Lanois, P. [Paul]. (2011). Privacy in the age of the cloud. *Journal of Internet law*, 15(6), 3–17.
- Lynskey, O. [Orla]. (2014). Deconstructing data protection: The “added-value” of a right to data protection in the eu legal order. *International and Comparative Law Quarterly*, 63(3), 569–597.
- Lynskey, O. [Orla]. (2017). The ‘Europeanisation’ of Data Protection Law. *Cambridge Yearbook of European Legal Studies*, 19, 252–286.
- Manatt, Phelps & Phillips LLP. (15 June 2022). *Congress Releases Draft American Data Privacy and Protection Act*. <https://www.jdsupra.com/legalnews/congress-releases-draft-american-data-6894033>.
- Margulies, P. [Peter]. (2014). The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism. *Fordham International Law Review*, 82(5), 2137–2167.
- Ohm, P. [Paul]. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, Vol. 57, 1701–1777.
- Pipe, R. [Russell]. (1984). International information policy: Evolution of transborder data flow issues. *Telematics*, 1(4), 409–418.
- Pouillet, Y. [Yves]. (2009). Data protection legislation: What is at stake for our society and democracy?. *Computer Law & Security Review*, 25(3), 211–226.
- Prosser, W. [William]. (1960). Privacy. *California Law Review*, 48(3), 383–423.
- Reidenberg, J. [Joel]. (1996). Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*, 45, 911–930.
- Reidenberg, J. [Joel]. (2001). E-Commerce and trans-atlantic privacy. *Houston Law Review*, 2001, 717–749.
- Robinson, N. [Neil]. (2009). Has European Data Protection Law Become Outdated? *Zeitschrift für Multimedia und Recht*, 2009(11), 725–726.
- Roch, M. P. [Michael P.]. (1996). Filling the Void of Data Protection in the United States: Following the European Example. *Santa Clara Computer and High Technology Law Journal*, 12(1), 71–96.
- Rojszczak, M. [Marcin]. (2020). CLOUD act agreements from an EU perspective. *Computer Law & Security Review*, 38 (2020), <https://doi.org/10.1016/j.clsr.2020.105442>.
- Rojszczak, M. [Marcin]. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, 29(1), 22–44.
- Roßnagel, A. [Alexander]. (2019). Kein “Verbotssprinzip” und kein “Verbot mit Erlaubnisvorbehalt” im Datenschutzrecht. *Neue Juristische Wochenschrift*, 72(1), 1–5.
- Roßnagel, A. [Alexander]. (2021). Grundrechtsschutz in der Datenwirtschaft. *Zeitschrift für Rechtspolitik*, 54(6), 173–176.
- Roßnagel, A. [Alexander]. (2014). Fahrzeugdaten – wer darf über sie entscheiden?. *Straßenverkehrsrecht*, 2014(8), 281–287
- Sacco, R. [Rodolfo]. (1991). Legal Formants: A Dynamic Approach to Comparative Law. *The American Journal of Comparative Law*, 39(1), 1–34.
- Schermer, B. [Bart]. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1), 45–52.
- Scholz, M. [Matthias] and Lutz, H. [Holger]. (2011). Standardvertragsklauseln für Auftragsdatenverarbeiter und § 11 BDSG Ein Plädoyer für die Unanwendbarkeit der §§ 11 Abs. 2, 43 Abs. 1 Nr. 2b) BDSG auf die Auftragsverarbeitung außerhalb des EWR. *Computer und Recht*, 27(7), 424–428.
- Schröder, C. [Christian] and Haag, N. [Nils]. (2011). Neue Anforderungen an Cloud Computing für die Praxis. *Zeitschrift für Datenschutz*, 2011(4), 147–152.
- Schulz, S. [Sebastian]. (2012). Privacy by Design. *Computer und Recht*, 28(3), 204–208.
- Schwartz, P. [Paul] and Solove, D. [Daniel]. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 86(6), 1814–1894.
- Schwartz, P. [Paul]. (2011). Personenbezogene Daten aus internationaler Perspektive. *Zeitschrift für Datenschutz*, 2011(3), 97–98.
- Sloan, M. [Michael]. (2010). Aristotle’s Nicomachean Ethics as the Original Locus for the Septem Circumstantiae. *Classical Philology*, 105(3), 236–251.
- Solove, D. [Daniel]. (2007). ‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy. *San Diego Law Review*, Vol. 44, 745–772.
- Spies, A. [Axel]. (2021). EU-US-Privacy-Shield – eine schwierige Reparatur. *Zeitschrift für Datenschutz*, 2021(9). 478–481. P. 481.

- Spies, A. [Axel]. (2020). Schrems-II-Urteil des EuGH und die USA: Mehr Licht!. *Zeitschrift für Datenschutz*, 2020(11), 549–550.
- Svantesson, D. J. B. [Dan Jerker B.]. (2015). Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*, 5(4), 226–234.
- Svantesson, D. J. B. [Dan Jerker B.]. (2013). A “layered approach” to the extraterritoriality of data privacy laws. *International Data Privacy Law*, 3(4), 278–286.
- Svantesson, D. J. B. [Dan Jerker B.]. (2015). The (uncertain) future of online data privacy. *Masaryk University Journal of Law and Technology*, 9(1), 129–153.
- Teubner, G. [Gunther]. (1996). Globale Bukowina: Zur Emergenz eines transnationalen Rechtspluralismus. *Rechtshistorisches Journal* 15, 1996, 255–290.
- Traung, P. [Peter]. (2012). The proposed new EU general data protection regulation. *Computer Law Review International*, 13(2), 33–49.
- Tzanou, M. [Maria]. (2013). Data protection as a fundamental right next to privacy? ‘Reconstructing’ a not so new right. *International Data Privacy Law*, 3(2), 88–99.
- van der Sloot, B. [Bart]. (2014). Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, 4(4), 307–325.
- Voigt, P. [Paul]. (2012). Auftragsdatenverarbeitung mit ausländischen Auftragnehmern - Geringere Anforderungen an die Vertragsausgestaltung als im Inland?. *Zeitschrift für Datenschutz*, 2012(12), 546–550.
- Voigt, P. [Paul]. Weltweiter Datenzugriff durch US-Behörden – Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten. *MMR* 2014(3), 148–161.
- Walker, N. [Neil]. (2008). Beyond Boundary Disputes and Basic Grids: Mapping the Global Disorder of Normative Orders. *International Journal of Constitutional Law*, 6(3-4), 373–396.
- Weber, M. [Marc] and Voigt, P. [Paul]. (2011). Internationale Auftragsdatenverarbeitung - Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln. *Zeitschrift für Datenschutz*, 2011(2), 74–78.
- Weber, R. [Rolf]. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, Vol. 3(2), 117–130.
- Weichert, T. [Thilo]. (2013). Big Data und Datenschutz. Chancen und Risiken einer neuen Form der Datenanalyse. *Zeitschrift für Datenschutz*, 2013(6), 251–259.

9. Online articles

- Aaronson, S.A. [Susan Ariel]. (2018). Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows. *Centre for International Governance Innovation Papers*, No. 197. https://www.cigionline.org/static/documents/documents/paper%20no.197_0.pdf
- Boullenois, C. [Camille]. (October 2021). China’s Data Strategy. In *European Union Institute for Security Studies*, Brief 21, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf.
- Engel, C. [Christoph]. (21 August 2002). *The Role of Law in the Governance of the Internet*. <http://dx.doi.org/10.2139/ssrn.325362>.
- Fischer, P. E. [Philipp Eberhard]. (2012). Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing. *JIPITEC*, 3(1), 33–59. <https://www.jipitec.eu/issues/jipitec-3-1-2012/3321/fischer.pdf>.
- Greenleaf, G. [Graham] and Clarke, R. [Roger] and Waters, N. [Nigel]. (27 September 2013). International Data Privacy Standards: A Global Approach (Australian Privacy Foundation Policy Statement), *UNSW Law Research Paper No. 2013-62*, <http://dx.doi.org/10.2139/ssrn.2327325>.
- Greenleaf, G. [Graham]. (1 October 2021). China’s Completed Personal Information Protection Law: Rights Plus Cyber-security. *Privacy Laws & Business International Report*, 2021(172), <https://ssrn.com/abstract=3989775>.
- Greenleaf, G. [Graham]. (9 April 2018). The UN Should Adopt Data Protection Convention 108 as a Global Treaty. *UNSW Law Research Paper*, 18(24), <https://ssrn.com/abstract=3159846>.
- Kuner, C. [Christopher]. (16 April 2021). Territorial Scope and Data Transfer Rules in the GDPR: Realizing the EU’s Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper No. 20/2021*, <http://dx.doi.org/10.2139/ssrn.3827850>.
- Kuner, C. [Christopher]. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD iLibrary*, No. 187. <https://doi.org/10.1787/5kg0s2fk315f-en>.
- Solove, D. [Daniel] and Keats Citron, D. [Danielle]. (2022). *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*. 101 Boston University Law Review Online 62 (2021), GWU Legal Studies Research Paper No. 2022-06, GWU Law School Public Law Research Paper No. 2022-06, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895191.
- Tosza, S. [Stanislaw]. (19 September 2019). *Mutual Recognition by Private Actors in Criminal Justice? Service Providers As Gatekeepers of Data and Human Rights Obligations*, <https://ssrn.com/abstract=3517878>.
- Trakman, L. [Leon] and Walters, R. [Robert] and Zeller, B. [Bruno]. (2019). Is Privacy and Personal Data Set to Become the New Intellectual Property?. *International Review of Intellectual Property and Competition Law*, 937–970, <http://dx.doi.org/10.2139/ssrn.3448959>.

Waldrop, M. [Mitch]. (2015). DARPA and the Internet Revolution. *Defense Advanced Research Projects Agency, 2015*, 78–85. [https://www.darpa.mil/attachments/\(2015\)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20\(Approved\).pdf](https://www.darpa.mil/attachments/(2015)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf)

10. Blogs

Bradford Franklin, S. [Sharon] and Sarkesian, L. [Lauren]. (7 April 2021). Strengthening Surveillance Safeguards After Schrems II. *New America*. <https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii>.

Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (16 February 2022). EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers. *European Law Blog*. <https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers>.

Christakis, T. [Theodore] and Propp, K. [Kenneth] and Swire, P. [Peter]. (31 January 2022). EU/US Adequacy Negotiations and the Redress Challenge: EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an “Essentially Equivalent” Solution. *European Law Blog*. <https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution>.

Creemers, R. [Rogier] and Triolo, P. [Paul] and Webster, G. [Graham]. (29 June 2018). Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017). *New America*. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china>.

Hogarth, I. [Ian]. (13 June 2018). AI Nationalism. *Ian Hogarth*. <https://www.ianhogarth.com/blog/2018/6/13/ai-nationalism>.

Kloth, A. [Alexander]. (5 February 2018). One law to rule them all, On the extraterritorial applicability of the new EU General Data Protection Regulation. *Völkerrechtsblog*. <https://voelkerrechtsblog.org/de/one-law-to-rule-them-all>.

Matthiesen, R. [Reemt] and Heinzke, P. [Philippe] and Dreyer, J. [Julia]. (9 April 2021). Schrems II: Reaktionen auf das Urteil und Empfehlungen der Aufsichtsbehörden – Update #23. *CMS Deutschland*. <https://www.cms-shs-bloggt.de/tmc/datenschutzrecht/schrems-ii-aufsichtsbehoerde-standardvertragsklausel-scc>.

Medium Corporation. (2018, 3 December). Extraterritorial application of the GDPR [blog post]. *Golden Data Law*. <https://medium.com/golden-data/extraterritorial-application-of-the-gdpr-fff3dfbb8c4>

11. Web pages

Aaronson, S.A. [Susan Ariel]. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*. <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows>.

Adams, S. [Samuel]. (26 April 2022). *Virginia amendment process complete, text finalized, ahead of Jan. 1 effective date*. <https://iapp.org/news/a/vcdpa-amendment-process-complete-text-finalized-ahead-of-jan-1-effective-date>.

Albus, V. [Valerie]. (15 June 2023). *Fast-Tracking Law Enforcement at the Expense of Fundamental Rights*. <https://verfassungsblog.de/fast-tracking-law-enforcement-at-the-expense-of-fundamental-rights>.

Alexander, F. [Filip]. (2017). *Internationale Datentransfers - Sicht einer deutschen Aufsichtsbehörde*. <https://docplayer.org/113788840-Internationale-datentransfers-sicht-einer-deutschen-aufsichtsbehoerde.html>.

American Chamber of Commerce to the European Union. (30 July 2020). *Joint Industry Letter on Schrems II Case Ruling*. <https://www.itic.org/policy/JointIndustryLetterSchremsII-30July.pdf>.

American Civil Liberties Union. (2 July 2014). *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. <https://www.aclu.org/other/pclp-report-surveillance-pursuant-section-702>.

American Civil Liberties Union. (23 October 2001). *Surveillance Under the USA/Patriot Act*. <https://www.aclu.org/other/surveillance-under-usapatriot-act>.

American Civil Liberties Union. (February 2015). *Informational Privacy in the Digital Age, A Proposal to Update General Comment 16 (Right to Privacy) to the International Covenant on Civil and Political Rights, A Report by the American Civil Liberties Union*. https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf.

Amnesty International. (27 May 2022). *Annual Report 2002*. <https://www.amnesty.org/download/Documents/POL1000012002ENGLISH.PDF>.

APEC. (March 2020). *Regulations, Policies and Initiatives on E-Commerce and digital economy for APEC MSMEs’ Participation in the Region*. https://www.apec.org/docs/default-source/publications/2020/3/regulations-policies-and-initiatives-on-e-commerce-and-digital-economy/220ecsgregulations-policies-and-initiatives-on-ecommerce-and-digital-economy-for-apec-msmes-particip.pdf?sfvrsn=63b748d7_1.

Article 29 Working Party. (11 April 2018). *Sorry is not enough: WP29 establishes a Social Media Working Group*. https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf.

Article 29 Working Party. (16 October 2015). *Statement of the Article 29 Working Party*. https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

- Article 29 Working Party. (23 November 2006). *Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2006/pr_swift_affair_23_11_06_en.pdf.
- Article 29 Working Party. (28 November 2014). *Letter of 28 November 2014 to the Cybercrime Convention Committee*. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20141128__letter_of_the_art_29_wp_t-cy_on_the_cybercrime_scenarios__not_signed.pdf.
- Artzt, M. [Matthias] and Delacruz, W. [Walter]. (29 January 2019). *How to comply with both the GDPR and the CLOUD Act*. <https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act>.
- Asia-Pacific Economic Cooperation. (2023). *Member Economies*. <https://www.apec.org/About-Us/About-APEC/Member-Economies.aspx>.
- Association of Southeast Asian Nations (ASEAN) and European Commission. (2023). *Joint guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*. <https://asean.org/wp-content/uploads/2023/05/The-Joint-Guide-to-ASEAN-Model-Contractual-Clauses-and-EU-Standard-Contractual-Clauses.pdf>.
- Australian Government, Department of Foreign Affairs and Trade. (16 July 2023). *Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)*. <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership>.
- Auswärtiges Amt und Bundesministerium der Justiz. (19 July 2013). *Letter of 19 July 2013*. https://cdn.netzpolitik.org/wp-upload/2013-07-19_AA_BMJ_Aussen_Justiz.pdf.
- Autoriteit Persoonsgegevens. (2023). *Bekijk binnen het onderwerp Cookies*. <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#hoe-kan-ik-bij-google-analytics-de-privacy-van-mijn-websitebezoekers-beschermen-4898>.
- BakerMcKenzie. (3 August 2021). *Standardizing data processing agreements globally, Webinar*. https://f.datasrvr.com/fr1/321/63074/Standardizing_Data_Processing_Agreements_Globally.pdf.
- Ballotpedia. (3 November 2020). *California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*. [https://ballotpedia.org/California_Consumer_Personal_Information_Law_and_Agency_Initiative_\(2020\)](https://ballotpedia.org/California_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020)).
- Bauer, M. [Matthias] and Ferracane, M. [Martina] and Lee-Makiyama, H. [Hosuk] and van der Mare, E. [Erik]. (December 2016). *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localization Measures in the EU Member States*. <https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu>.
- Bertuzzi, L. [Luca]. (1 October 2021). *EU countries green light new data governance framework*. <https://www.euractiv.com/section/data-protection/news/eu-countries-green-light-new-data-governance-framework>.
- Bertuzzi, L. [Luca]. (9 February 2022). *Inside the EU's rocky path to regulate artificial intelligence*. <https://iapp.org/news/a/inside-the-eus-rocky-path-to-regulate-artificial-intelligence>.
- Bertuzzi, L. [Luca]. (14 April 2022). *DMA: significant additions made it into the final text*. <https://www.euractiv.com/section/digital/news/dma-significant-additions-made-it-into-the-final-text>.
- Bertuzzi, L. [Luca]. (19 October 2022). *EU Council nears common position on AI Act in semi-final text*. <https://www.euractiv.com/section/digital/news/eu-council-nears-common-position-on-ai-act-in-semi-final-text>.
- Bertuzzi, L. [Luca]. (28 June 2022). *10 years after: The EU's 'crunch time' on GDPR enforcement*. <https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement>.
- Bitkom. (15 September 2021). *Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers*. <https://www.bitkom.org/sites/default/files/2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf>.
- Boehm, F. [Franziska]. (August 2018). *Legal Expertise on the adequacy of the Privacy Shield*. https://www.zar.kit.edu/DATA/veroeffentlichungen/237_Attachment_8_-_Expert_Review_by_Prof._Franziska_Boehm_a246a66.pdf.
- Boyce, A. [Antonia] and Hutt, L. [Louise] and Boardman, R. [Ruth]. (May 2021). *Article 49 Derogations – Summary Table with Examples*. <https://iapp.org/resources/article/article-49-derogations-summary-table-with-examples>.
- Bracy, J. [Jedidiah]. (12 April 2022). *Apple's Tim Cook: Protecting privacy most essential battle of our time*. <https://iapp.org/news/a/apples-tim-cook-protecting-privacy-most-essential-battle-of-our-time>.
- Bracy, J. [Jedidiah]. (7 July 2022). *Irish DPC files draft order to halt Meta's data transfers to US*. <https://iapp.org/news/a/irish-dpc-files-draft-order-to-halt-metas-data-transfers-to-us>.
- Brandon LaLonde, B. [Brandon] and Thompson, M. [Mark] and Kanthasamy, S. [Saz]. (2021). *IAPP-EY Annual Privacy Governance Report 2021*. <https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2021>.
- Brennan Center for Justice. (15 July 2013). *Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs*. <https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf>.
- Brill, J. [Julia]. (25 March 2022). *EU-U.S. data agreement an important milestone for data protection, Microsoft is committed to doing our part*. <https://blogs.microsoft.com/eupolicy/2022/03/25/eu-us-data-agreement-an-important-milestone-for-data-protection-microsoft-is-committed-to-doing-our-part>.
- Bryant, J. [Jennifer]. (20 January 2022). *Austrian DPA's Google Analytics decision could have "far-reaching implications"*. <https://iapp.org/news/a/far-reaching-implications-anticipated-with-austrian-dpas-google-analytics-decision>.
- Bryant, J. [Jennifer]. (24 July 2023). *EU-US Data Privacy Framework adopted, what now?*. <https://iapp.org/news/a/eu-us-data-privacy-framework-adopted-what-now>.
- Bryant, J. [Jennifer]. (28 June 2022). *Google Analytics enforcement fallout: 'Cry and pray'*. <https://iapp.org/news/a/google-analytics-enforcement-fallout-cry-and-pray>.

- Bryant, J. [Jennifer]. (9 June 2022). *CPA board moves CPRA rulemaking process forward*. <https://iapp.org/news/a/cpa-board-launches-cpra-rulemaking-process>.
- Bundeskartellamt. (7 February 2019). *Bundeskartellamt prohibits Facebook from combining user data from different sources*. https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2.
- Cambridge Dictionary. (2023). *cross-border*. <https://dictionary.cambridge.org/dictionary/english/cross-border>.
- Castro, D. [Daniel]. (6 June 2022). *Review of the Proposed “American Data Privacy and Protection Act, Part 1: State Preemption and Private Right of Action*. <https://itif.org/publications/2022/06/06/american-data-privacy-and-protection-act-review-part-1-state-preemption-and-private-right-of-action>.
- Castro, D. [Daniel]. (13 June 2022). *A Review: The American Data Privacy and Protection Act*. <https://www.govtech.com/policy/a-review-the-american-data-privacy-and-protection-act>.
- Castro, D. [Daniel] and Dascoli, L. [Luke] and Diebold, G. [Gillian]. (24 January 2022). *The Looming Cost of a Patchwork of State Privacy Laws*. <https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws>.
- Cavoukian, A. [Ann]. (8 November 2006). *Creation of Global Privacy Standard*. https://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf.
- Cavoukian, A. [Ann]. (January 2011). *Privacy by Design. The 7 Foundational Principles*. <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>
- Chen, L. [Lurong] et al. (2019). *The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies*. <https://t20japan.org/policy-brief-digital-economy-economic-development>.
- Christakis, T. [Theodore]. (14 January 2019). *E-Evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead*. <https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/?cn-reloaded=1>.
- Clyde&Co. (28 October 2021). *Brief review of the Data Security Law*. <https://www.clydeco.com/en/insights/2021/10/brief-review-of-the-data-security-law>.
- CNET. (14 September 2007). *Google proposes global privacy standard*. http://news.cnet.com/Google-proposes-global-privacy-standard/2100-1030_3-6207927.html.
- CNET. (2 January 2022). *Congress fears European privacy standards*. <https://www.cnet.com/tech/services-and-software/congress-fears-european-privacy-standards>.
- CNIL. (21 January 2019). *The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.
- CNIL. (6 January 2022). *Cookies: la CNIL sanctionne GOOGLE à hauteur de 150 millions d’euros et FACEBOOK à hauteur de 60 millions d’euros pour non-respect de la loi*. <https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions>.
- CoE. (16 September 2022). *Russia ceases to be party to the European Convention on Human Rights*. <https://www.coe.int/en/web/portal/-/russia-ceases-to-be-party-to-the-european-convention-on-human-rights>.
- CoE. (29 September 2020). *The EU’s accession to the European Convention on Human Rights*. <http://www.coe.int/en/web/portal/-/the-eu-s-accession-to-the-european-convention-on-human-rights>.
- Commission Nationale de l’Informatique et des Libertés. (10 February 2022). *Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply*. <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>.
- Commission Nationale de l’Informatique et des Libertés. (7 June 2022). *Questions-réponses sur les mises en demeure de la CNIL concernant l’utilisation de Google Analytics*. <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/questions-reponses-sur-les-mises-en-demeure-de-la-cnil-concernant-lutilisation-de-google-analytics>.
- Computer Weekly. (16 May 2022). *Europol gears up to collect big data on European citizens after MEPs vote to expand policing power*. <https://www.computerweekly.com/news/252518218/Europol-gears-up-to-collect-big-data-on-European-citizens-after-MEPs-vote-to-expand-policing-power>.
- Conference of German Independent Data Protection Supervisors of the Federal Government and the States. (15 November 2021). *Expert Opinion on the Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladek, University of Texas School of Law*. https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf. P. 8–9.
- Cooly LLP. (12 April 2022). *Cross-Border Data Transfers: PIPL vs. GDPR vs. CCPA*. <https://www.jdsupra.com/legalnews/cross-border-data-transfers-pipl-vs-9241114>.
- Cory, N. [Nigel] and Atkinson, R. [Robert] and Castro, D. [Daniel]. (27 May 2019). *Principles and policies for data free flow with trust*. <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust>.
- Cory, N. [Nigel] and Dascoli, L. [Luke]. (19 July 2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.
- Costigan J. [Johanna] and Webster, G. [Graham] (eds.). (March 2021). *14th five-year plan for the national economic and social development of the People’s Republic of China and the outline of long-term goals for 2035*. <https://digichina.stanford.edu/wp-content/uploads/2022/01/DigiChina-14th-Five-Year-Plan-for-National-Informatization.pdf>.

- Council of Europe. (16 March 2022). *The Russian Federation is excluded from the Council of Europe*. <https://www.coe.int/en/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe>.
- Council of Europe. (17 November 2021). *Cybercrime: Council of Europe strengthens its legal arsenal*. https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a48ca6.
- Council of Europe. (2023). *Convention 108 and Protocols*. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.
- Council of Europe. (23 June 2023). *Chart of signatures and ratifications of Treaty 223*. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures>.
- Council of Europe. (24 June 2023). *Chart of signatures and ratifications of Treaty 108*. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.
- Council of Europe. (28 July 2023). *Chart of signatures and ratifications of Treaty 181*. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=181>.
- Council of Europe. (5 April 2013). *Fifth Negotiation Meeting between the CD DH ad hoc Negotiation Group and the European Commission on the accession of the European Union to the European Convention on Human Rights*. http://www.echr.coe.int/Documents/UE_Report_CDDH_ENG.pdf.
- Council of Europe. (January 2016). *Analysis of statistics 2015*. http://www.echr.coe.int/Documents/Stats_analysis_2015_ENG.pdf. // Council of Europe. (January 2017).
- Council of Europe. (January 2017). *Analysis of statistics 2016*. http://www.echr.coe.int/Documents/Stats_analysis_2016_ENG.pdf.
- Council of Europe. (June 2020). *Supervision of the execution of judgements and decisions of the European Court of Human Rights 2019 - 13th Annual Report of the Committee of Ministers (2020)*. <https://edoc.coe.int/fr/convention-europenne-des-droits-de-l-homme/8176-supervision-of-the-execution-of-judgements-of-the-european-court-of-human-rights-2018-12th-annual-report-of-the-committee-of-ministers.html>.
- Council of Europe. *The modernized Convention 108: novelties in a nutshell*. <http://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8>.
- Council of the European Union. (15 February 2023). *Better access to e-evidence to fight crime*. <https://www.consilium.europa.eu/en/policies/e-evidence>.
- Council of the European Union. (16 May 2022). *Council approves Data Governance Act*. <https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees>.
- Council of the European Union. (20 September 2022). *Press Release No 158/2*. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158en.pdf>.
- Council of the European Union. (2023). *The ordinary legislative procedure*. <https://www.consilium.europa.eu/en/council-eu/decision-making/ordinary-legislative-procedure>.
- Council of the European Union. (30 November 2021). *Promoting data sharing: presidency reaches deal with Parliament on Data Governance Act*. <https://www.consilium.europa.eu/en/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act>.
- Council of the European Union. (6 June 2019). *Council gives mandate to Commission to negotiate international agreements on e-evidence in criminal matters*. <https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters>.
- Council of the European Union. (7 October 2019). *10th anniversary of the Charter of fundamental rights: Council reaffirms the importance of EU common values*. <https://www.consilium.europa.eu/en/press/press-releases/2019/10/07/10th-anniversary-of-the-charter-of-fundamental-rights-council-reaffirms-the-importance-of-eu-common-values>.
- Court of Justice of the European Union. (20 September 2022). *Press Release No 158/2*. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220158en.pdf>.
- Court of Justice of the European Union. (6 October 2015). *Press release no. 117/15. The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid*. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>.
- Crosby, D. [Daniel]. (March 2016). *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, International Centre for Trade and Sustainable Development (ICTSD)*. <https://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>.
- Cross Border Privacy Rules System. (2023). *Cross Border Privacy Rules System Directory*. <http://cbprs.org/compliance-directory/cbpr-system>.
- Cryptome. (2 November 2013). *NSA SSO1 Slide from Guardian 13-1101*. <https://cryptome.org/2013/11/nsa-sso1-guardian-13-1101.pdf>.
- ctrl+verlust, (23 March 2011). *Was ist Postprivacy (für mich)?*. <https://www.ctrl-verlust.net/was-ist-postprivacy-fur-mich>.
- Datatilsynet. (19 January 2022). *Afgørelse om brug af Google Analytics fra det østrigske datatilsyn*. <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jan/afgoerelse-om-brug-af-google-analytics-fra-det-oestrigske-datatilsyn>.
- Datatilsynet. (21 September 2022). *Brug af Google Analytics til webstatistik*. <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/brug-af-google-analytics-til-webstatistik>.

- Datenschutzbehörde der Republik Österreich. (22 December 2021). *Decision of 22 December 2021*. https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf.
- Datenschutzkonferenz. (31 January 2023). *Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 31. Januar 2023, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten*. https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf.
- de Hert, P. [Paul] and Schreuders, E. [Eric]. (2001). *The Relevance of Convention 108. European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future*. https://cris.vub.be/ws/portalfiles/portal/37771545/pdh2001_es_the_relevance_of_convention_108_.pdf.
- DE-CIX Management GmbH. (2022). *Traffic Frankfurt – 5 years*. <https://www.de-cix.net/en/locations/germany/frankfurt/statistics>.
- Dentons Kensington Swan. (19 July 2023). *Latest instalment in EU-US Data Protection Framework—will it stand?*. <https://www.dentons.co.nz/en/insights/articles/2023/july/17/latest-instalment-in-eu-us-data-protection-framework>.
- Der Spiegel. (11 June 2019). *Alle Daten an alle Staaten*. <https://www.spiegel.de/netzwelt/netzpolitik/e-evidence-warum-die-eu-plaene-zu-digitalen-beweisen-gefaehrlich-sind-a-1270939.html>.
- Desai, A. [Anokhy]. (7 July 2023). *US State Privacy Legislation Tracker*. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker>.
- Deutsche Telekom AG. (1 July 2020). *Position der Deutschen Telekom zur EU-Ratspräsidentschaft Deutschlands*. <https://www.telekom.com/resource/blob/608208/2524892254e198e89bf07a5cdf9c61be/dl-position-telekom-zur-eu-ratspraesidentschaft-deutschlands-data.pdf>.
- Deutscher Bundestag. (9 January 2020). *Umsetzung und Zeitplanung von "GAIA-X"*. <http://dip21.bundestag.de/dip21/btd/19/164/1916434.pdf>.
- Die Bundesregierung. (19 July 2013). *Sommerpressekonferenz von Bundeskanzlerin Merkel vom 19. Juli*. <https://www.bundeskanzler.de/bk-de/suche/sommerpressekonferenz-von-bundeskanzlerin-merkel-vom-19-juli-844124>.
- Dieffenbacher, S. F. [Stefan F.]. (4 March 2023). *Digitization vs Digitalization: Differences, Definitions, and Examples*. <https://digitalleadership.com/blog/digitization-vs-digitalization>.
- Diercks, N. [Nina] and Roth, M. [Markus]. (30 August 2021). *Data Transfer to unsafe Third Countries*. <https://www.wolterskluwer.com/en/expert-insights/data-transfer-to-unsafe-third-countries>.
- Drexl, J. [Josef] and Hilty, R. [Reto] et al. (16 August 2016). *Ausschließlichkeits- und Zugangsrechte an Daten, Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb vom 16. August 2016 zur aktuellen europäischen Debatte*. https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI-Stellungnahme_Daten_2016_08_16_final.pdf.
- Duball, J. [Joseph]. (2 June 2022). *US lawmakers closing in on bipartisan privacy framework*. <https://iapp.org/news/a/us-lawmakers-closing-in-on-bipartisan-privacy-framework>.
- Duball, J. [Joseph]. (3 September 2020). *LIBE meeting scrutinizes path forward for EU-US data transfers*. <https://iapp.org/news/a/libe-meeting-reveals-plan-scrutiny-of-path-forward-for-eu-us-data-transfers>.
- Duball, J. [Joseph]. (6 June 2022). *US lawmakers unveil bipartisan American Data Privacy and Protection Act*. <https://iapp.org/news/a/congress-unveils-american-data-privacy-and-protection-act>.
- Duball, J. [Joseph]. (21 July 2022). *American Data Privacy and Protection Act heads for US House floor*. <https://iapp.org/news/a/american-data-privacy-and-protection-act-heads-for-us-house-floor>.
- Duball, J. [Joseph]. (27 June 2022). *Roe v. Wade reversal sends ripples through privacy world*. <http://iapp.org/news/a/roe-v-wade-reversal-sends-ripples-through-privacy-world>.
- Duball, J. [Joseph]. (29 July 2022). *Calif. privacy agency takes aim at dismantling federal privacy preemption*. <https://iapp.org/news/a/cppa-takes-aim-at-dismantling-american-data-privacy-and-protection-acts-preemption>.
- Dutton, W. H. [William H.] and Peltu, M. [Malcolm]. (November 2005). *The Emerging Internet Governance Mosaic: Connecting the Pieces*. <http://dx.doi.org/10.2139/ssrn.1295330>.
- ECtHR, (1 June 2016). *The Interlaken process and the Court (2016 Report)*. https://www.echr.coe.int/Documents/2016_Interlaken_Process_ENG.pdf.
- ECtHR, (1 June 2016). *The Interlaken process and the Court (2016 Report)*. https://www.echr.coe.int/Documents/2016_Interlaken_Process_ENG.pdfhttps://www.echr.coe.int/Documents/2016_Interlaken_Process_ENG.pdf.
- Eggerton, J. [Jon]. (3 November 2021). *House Republicans Tag Team on Privacy Bill Draft*. <https://www.mediainstitute.org/2021/11/03/house-republicans-tag-team-on-privacy-bill-draft/>
- Electronic Frontier Foundation. (1 December 2016). *Fighting NSL Gag Orders, With Help From Our Friends at CREDO and Internet Archive*. <https://www.eff.org/de/deeplinks/2016/12/fighting-nsi-gag-orders-help-our-friends-credo-and-internet-archive>.
- Electronic Frontier Foundation. (10 July 2013). *International Principles on the Application of Human Rights to Communications Surveillance*. <https://www.eff.org/files/necessaryandproportionatefinal.pdf>.
- Electronic Frontier Foundation. (15 November 2013). *Memorandum OC-034-12*. https://www.eff.org/files/2013/11/15/20130816-wapo-sid_oversight.pdf.
- Electronic Frontier Foundation. (2023). *Decoding 702: What is Section 702?*. <https://www.eff.org/702-spying>.
- Electronic Frontier Foundation. (24 July 2014). *12333 flowchart*. <http://www.eff.org/files/2014/07/24/12333flowchart.pdf>.

- Electronic Frontier Foundation. (29 December 2020). *Section 215 Expired: Year in Review 2020*. <https://www.eff.org/de/deeplinks/2020/12/section-215-expired-year-review-2020>.
- Electronic Frontier Foundation. (30 November 2016). *CREDO Confirms It's at Center of Long-Running Legal Fight Over NSLs*. <https://www.eff.org/press/releases/credo-confirms-its-center-long-running-NSL-fight>.
- Electronic Frontier Foundation. (4 August 2017). *E-commerce RCEP Chapter: Have Big Tech's Demands Fizzled?*. <https://www.eff.org/deeplinks/2017/08/e-commerce-rcep-chapter-have-big-techs-demands-fizzled>.
- Electronic Privacy Information Center. (16 September 2015). *Re: Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015*. <https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf>.
- Electronic Privacy Information Center. (16 September 2015). *Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015*. <https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf>.
- Electronic Privacy Information Center. (2022). *FISA Orders: 1979-2020. FISA Court Orders and National Security Letters Issued*. <https://epic.org/privacy/surveillance/fisa/graphs>.
- Electronic Privacy Information Center. (7 May 1998). *Testimony and Statement for the Record of Marc Rotenberg on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives*. <https://epic.org/privacy/intl/rotenberg-eu-testimony-598.html>.
- Electronic Privacy Information Center. (January 2005). *The Gramm-Leach-Bliley Act*. <http://epic.org/privacy/glbs/default.html>.
- Ethyca Inc. (2023). *About*. <https://ethyca.com/about>.
- European Centre for International Political Economy. (December 2016). *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localization Measures in the EU Member States*. <https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu>.
- European Centre for International Political Economy. (March 2013). *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*. https://www.uschamber.com/assets/archived/images/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.
- European Commission. (10 January 2017). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication*. <https://digital-strategy.ec.europa.eu/en/library/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector>.
- European Commission. (10 May 2022). *Questions and Answers: Digital Services Act*. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348.
- European Commission. (11 April 2023). *Adequacy decisions*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
- European Commission. (14 April 2016). *Joint Statement on the final adoption of the new EU rules for personal data protection*. http://europa.eu/rapid/press-release_STATEMENT-16-1403_de.htm.
- European Commission. (14 July 2016). *EU negotiating texts in TTIP*. <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1230>.
- European Commission. (15 December 2020). *Europe fit for the Digital Age: Commission proposes new rules for digital platforms*. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2347.
- European Commission. (18 October 2017). *EU-U.S. Privacy Shield: First review shows it works but implementation can be improved*. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3966.
- European Commission. (19 December 2016). *ePrivacy: consultations show confidentiality of communications and the challenge of new technologies are key questions*. <https://wayback.archive-it.org/12090/20190630043525/https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-communications-and-challenge-new-technologies-are>.
- European Commission. (20 March 2019). *Antitrust: Commission fines Google EUR 1.49 billion for abusive practices in online advertising*. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.
- European Commission. (2018). *Improving cross-border access to electronic evidence in criminal matters*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1453-Improving-cross-border-access-to-electronic-evidence-in-criminal-matters_en.
- European Commission. (2019). *E-evidence - cross-border access to electronic evidence*. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.
- European Commission. (2020). *Data protection - standard contractual clauses between controllers & processors located in the EU (implementing act)*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Data-protection-standard-contractual-clauses-between-controllers-processors-located-in-the-EU-implementing-act_en.
- European Commission. (2020). *Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act)*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act_en.
- European Commission. (2020). *Police cooperation – stronger mandate for Europol*. Ref. Ares(2020)2555219. <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate>.
- European Commission. (2021). *Data sharing in the EU – common European data spaces (new rules)*. <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Legislative-framework-for-the-governance-of-common-European-data-spaces>.

- European Commission. (2022). *Bessere Rechtsetzung – warum und wie?*. https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation_de.
- European Commission. (2023). *A European Green Deal*. https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.
- European Commission. (2023). *NIFO - National Interoperability Framework Observatory*. <https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/1-introduction#1.1>.
- European Commission. (2023). *Strategic foresight*. https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight_en.
- European Commission. (2023). *The Digital Services Act package*. <https://ec.europa.eu/digital-single-market/en/digital-services-act-package>.
- European Commission. (23 February 2022). *Data Act – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114.
- European Commission. (23 February 2022). *Data Act: Commission proposes measures for a fair and innovative data economy*. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.
- European Commission. (24 February 2023). *Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en.
- European Commission. (24 January 2020). *WP225 Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12*. <https://ec.europa.eu/newsroom/article29/redirection/document/64437>.
- European Commission. (25 April 2016). *EU Criminal Law – key to a Security Union based on fundamental rights and values*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_16_1582.
- European Commission. (25 May 2022). *Questions and Answers for the two sets of Standard Contractual Clauses*. https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf.
- European Commission. (25 November 2020). *Commission proposes measures to boost data sharing and support European data spaces*. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2102.
- European Commission. (27 November 2013). *Speech - EU-US agreements: Commission reports on TFTP and PNR*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_13_985.
- European Commission. (27 September 2019). *Security Union: The Commission recommends opening negotiations with Japan on the transfer of Passenger Name Record (PNR) data*. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5872.
- European Commission. (28 January 2014). *Speech: A data protection compact for Europe*. https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_14_62.
- European Commission. (4 November 2010). *European Commission sets out strategy to strengthen EU data protection rules*. https://ec.europa.eu/commission/presscorner/detail/en/IP_10_1462.
- European Commission. (5 February 2019). *Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention*. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_865.
- European Commission. (5 February 2019). *Security Union: Commission recommends negotiating international rules for obtaining electronic evidence*. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_843.
- European Commission. (5 June 2020). *Border & law enforcement - advance passenger information (API) - revised rules*. https://ec.europa.eu/home-affairs/what-is-new/work-in-progress/initiatives/border-law-enforcement-advance-passenger-information-api-revised-rules_en.
- European Commission. (6 May 2015). *A Digital Single Market Strategy for Europe - Analysis and Evidence*. SWD (2015) 100 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0100&from=EN>.
- European Commission. (6 November 2015). *Q&A: Guidance on transatlantic data transfers following the Schrems ruling*. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_6014.
- European Commission. (8 December 2020). *Answer given by Mr Reynders on behalf of the European Commission, E-004472/2020*. https://www.europarl.europa.eu/doceo/document/E-9-2020-004472-ASW_EN.pdf.
- European Commission. (8 September 2015). *Questions and Answers on the EU-US data protection “Umbrella agreement”*. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5612.
- European Commission. (9 March 2021). *Europe’s Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983.
- European Commission. (February 2020). *Shaping Europe’s digital future*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.
- European Council. (18 February 2020). *EU-Japan PNR agreement: Council authorizes opening of negotiations*. <https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations>.
- European Data Protection Board. (14 January 2021). *EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf.
- European Data Protection Board. (14 September 2022). *EDPB adopts statement on European Police Cooperation Code & picks topic for next coordinated action*. https://edpb.europa.eu/news/news/2022/edpb-adopts-statement-european-police-cooperation-code-picks-topic-next-coordinated_en.
- European Data Protection Board. (15 February 2022). *Launch of coordinated enforcement on use of cloud by public sector*. https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en.

- European Data Protection Board. (21 January 2019). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.
- European Data Protection Board. (22 January 2021). *Letter of 22 January 2021, OUT2021-0004*. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letteronreviewpnrdirective.pdf.
- European Data Protection Board. (23 July 2020). *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*. https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjecuc31118_en.pdf.
- European Data Protection Board. (29 April 2022). *DPAs decide on closer cooperation for strategic files*. https://edpb.europa.eu/news/news/2022/dpas-decide-closer-cooperation-strategic-files_en.
- European Data Protection Supervisor. (1 April 2016). *The EU GDPR as a clarion call for a new global digital gold standard*. https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_de.
- European Data Protection Supervisor. (10 January 2022). *EDPS orders Europol to erase data concerning individuals with no established link to a criminal activity*. https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en.
- European Data Protection Supervisor. (12 February 2016). *Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences, Opinion 1/2016*. https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf.
- European Data Protection Supervisor. (14 September 2021). *EUDPR: Conditions and Safeguards in International Transfers to Private Entities*. https://edps.europa.eu/system/files_en?file=2022-04/0167_2021-1047_01_redacted.pdf.
- European Data Protection Supervisor. (2 April 2019). *Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence, Opinion 2/2019*. https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e_evidence_en.pdf.
- European Data Protection Supervisor. (2023). *Data Protection*. https://edps.europa.eu/data-protection/data-protection_en.
- European Data Protection Supervisor. (6 November 2019). *EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters, Opinion 7/2019*. https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf.
- European Digital Rights and Privacy International. (5 December 2018). *Growing concerns on "e-evidence": Council publishes its draft general approach*. <https://edri.org/growing-concerns-on-e-evidence-council-publishes-draft-general-approach>.
- European Digital Rights and Privacy International. (5 February 2023). *e-Evidence compromise blows a hole in fundamental rights safeguards*. <https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards>.
- European Digital Rights and Privacy International. (6 July 2022). *Mass surveillance of external travellers may go on, says EU's highest court*. <https://edri.org/our-work/mass-surveillance-of-external-travellers-may-go-on-says-eus-highest-court/>.
- European Parliament. (11 February 2010). *SWIFT: European Parliament votes down agreement with the US*. <http://www.europarl.europa.eu/sides/getDoc.do?language=en&type=IM-PRESS&reference=20100209IPR68674>.
- European Parliament. (13 July 2011). *Question for written answer E-006901/2011*. http://www.europarl.europa.eu/doceo/document/E-7-2011-006901_EN.html.
- European Parliament. (14 June 2023). *MEPs ready to negotiate first-ever rules for safe and transparent AI*. <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>.
- European Parliament. (2023). *About LIBE*. <https://www.europarl.europa.eu/committees/en/libe/about>.
- European Parliament. (22 October 2013). *EP to vote on suspending SWIFT deal after committee vote on data protection*. <http://www.europarl.europa.eu/news/en/news-room/20131021STO22709/EP-to-vote-on-suspending-SWIFT-deal-after-committee-vote-on-data-protection>.
- European Parliament. (23 October 2013). *MEPs call for suspension of EU-US bank data deal in response to NSA snooping*. <https://www.europarl.europa.eu/news/en/press-room/20131021IPR22725/meps-call-for-suspension-of-eu-us-bank-data-deal-in-response-to-nsa-snooping>.
- European Parliament. (24 March 2022). *Deal on Digital Markets Act: EU rules to ensure fair competition and more choice for users*. <https://www.europarl.europa.eu/news/de/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users>.
- European Parliament. (25 November 2014). *MEPs refer EU-Canada air passenger data deal to the EU Court of Justice*. <http://www.europarl.europa.eu/news/en/press-room/20141121IPR79818/meps-refer-eu-canada-air-passenger-data-deal-to-the-eu-court-of-justice>.
- European Parliament. (26 May 2016). *Geplanter EU-US-Datenschutzschild verbesserungswürdig*. <http://www.europarl.europa.eu/news/de/press-room/20160524IPR28820/geplanter-eu-us-datenschutzschild-verbesserungswurdig>.
- European Parliament. (4 June 1999). *Cologne European Council, Conclusions of the Presidency*. https://www.europarl.europa.eu/summits/kol2_en.htm.

- European Parliament. (4 May 2022). *Parliament backs giving more powers to Europol, but with supervision*. <https://www.europarl.europa.eu/news/en/press-room/20220429IPR28234/parliament-backs-giving-more-powers-to-europol-but-with-supervision>.
- European Parliament. (7 December 2000). *European Council – Nice, Conclusions of the Presidency, 7 - 10 June 2000*. https://www.europarl.europa.eu/summits/nice1_en.htm.
- European Parliament. (July 2020). *Digital sovereignty for Europe*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).
- European Parliament. *Digital: The EU must set the standards for regulating online platforms, say MEPs*. (20 October 2020). <https://www.europarl.europa.eu/news/en/press-room/20201016IPR89543/digital-eu-must-set-the-standards-for-regulating-online-platforms-say-meps>.
- European Union Agency for Cybersecurity. (22 December 2020). *EUCS – Cloud Services Scheme*. <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>.
- europe-v-facebook.org. (25 June 2013). *Complaint against Facebook Ireland Ltd – 23 “PRISM”*. <http://www.europe-v-facebook.org/prism/facebook.pdf>.
- europe-v-facebook.org. (25 May 2016). *Rapid Press Update: Facebook & NSA-Surveillance: Following “Safe Harbor” decision, Irish Data Protection Commissioner to bring EU-US data flows before CJEU again*. http://www.europe-v-facebook.org/PA_MCs.pdf.
- europe-v-facebook.org. (27 November 2015). *Letter by Mason Hayes & Curran*. http://www.europe-v-facebook.org/comp_fb_scc.pdf.
- Feathers, T. [Todd]. (15 April 2021). *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*. <https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious>.
- Federal Trade Commission. (2021). *WFTC Staff Report Finds Many Internet Service Providers Collect Troves of Personal Data, Users Have Few Options to Restrict Use*. <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-staff-report-finds-many-internet-service-providers-collect-troves-personal-data-users-have-few>.
- Federal Trade Commission. (25 June 2009). *Fair Information Practice Principles*. <https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm>.
- Felz, D. [Daniel] and Swire, P. [Peter]. (15 December 2021). *New EU data blockage as German court would ban many cookie management providers*. <https://iapp.org/news/a/new-eu-data-blockage-as-german-court-would-ban-many-cookie-management-providers>.
- Ferracane, M. [Martina]. (November 2017). *Restrictions to Cross-Border Data Flows: a Taxonomy*. <https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy>.
- Fondazione Giacomo Brodolini. (1 December 2018). *Fundamental rights review of EU data collection instruments and programmes, final report*. https://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf.
- Fukunari, K. [Kimura]. (7 January 2020). *Developing a policy regime to support the free flow of data: A proposal by the T20 Task Force on Trade, Investment and Globalization*. <https://cepr.org/voxeu/columns/developing-policy-regime-support-free-flow-data-proposal-t20-task-force-trade>.
- Gain, V. [Vish]. (1 June 2023). *Microsoft says Irish DPC intends to slam LinkedIn with a \$425m fine*. <https://www.siliconrepublic.com/business/microsoft-linkedin-fine-irish-data-protection-commission-gdpr-draft>.
- Garante per la protezione dei dati personali*. (23 June 2022). *Google: Garante privacy stop all'uso degli Analytics. Dati trasferiti negli Usa senza adeguate garanzie*. <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9782874#english>.
- Gartner, Inc. (2023). *Gartner Glossary – Big Data*. <https://www.gartner.com/en/information-technology/glossary/big-data>.
- Geist, M. [Michael]. (4 April 2018). *Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. A CIGI Essay Series on Data Governance in the Digital Age*. https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security/?utm_source=twitter&utm_medium=social&utm_campaign=data-series.
- German Federal Foreign Office. (19 December 2013). *German Brazilian resolution on internet privacy adopted*. <https://www.auswaertiges-amt.de/en/aussenpolitik/internationale-organisationen/vereintenationen/131127-resolution-privatsphaere-im-internet/258450>.
- German Federal Ministry of the Interior. (10 October 2019). *Gutachten der Datenethikkommission*. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.
- Global Network Initiative. (2022). *About*. <https://globalnetworkinitiative.org>.
- Global Privacy Enforcement Network. (23 July 2023). *Members*. <https://www.privacyenforcement.net/content/members>.
- Google LLC. (6 February 2015). *The Advisory Council to Google on the Right to be Forgotten*. <https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf>.
- Google Public Policy Blog. (14 September 2007). *Call for global privacy standards*. <https://publicpolicy.googleblog.com/2007/09/call-for-global-privacy-standards.html>.
- Government of Canada. (2023). *Canada and the Asia-Pacific Economic Cooperation (APEC)*. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/apec/index.aspx?lang=eng.

- Greenberg, P. [Pam]. (27 December 2021). *2021 Consumer Data Privacy Legislation*. <https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx>.
- GSMA. (July 2019). *Operationalizing the ASEAN Framework on Digital Data Governance. A Regulatory Pilot Space for Cross-Border Data Flows*. https://www.gsma.com/asia-pacific/wp-content/uploads/2019/11/Operationalising-the-ASEAN-Framework-on-Digital-Data-Governance_WEB.pdf.
- GSMA. (September 2018). *Cross-Border Data Flows Realizing benefits and removing barriers*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf.
- GSMA. (September 2018). *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC can Protect Data and Drive Innovation*. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.
- Gstrein, O. [Oskar]. (28 May 2018). *Surveillance, Security, Privacy: What direction to reach the end of the tunnel?*. <https://www.juwiss.de/51-2018>.
- Henning, M. [Maximilian]. (9 March 2021). *Digitalwirtschaften ärmerer Länder sollen weiter schutzlos bleiben*. <https://netzpolitik.org/2021/verhandlungen-bei-der-wto-digitalwirtschaften-aermerer-laender-sollen-weiter-schutzlos-bleiben>.
- Heyder, M. [Markus]. (4 September 2014). *The APEC Cross-Border Privacy Rules—Now That We've Built It, Will They Come?*. <https://iapp.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come>.
- Ho, A. [Amelia]. (1 July 2018). *Roles of Three Lines of Defense for Information Security and Governance*. <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance>.
- Hogan Lovells. (12 July 2022). *China: updates on international data transfers*. <https://www.engage.hoganlovells.com/knowledgeservices/news/china-updates-on-international-data-transfers>.
- Hogan Lovells. (26 January 2022). *ASEAN Launches Model Contractual Clauses for Cross Border Data Transfers*. <https://www.jdsupra.com/legalnews/asean-launches-model-contractual-6923372>.
- Huld, A. [Arense]. (11 May 2022). *New Specifications for Cross-Border Processing of Personal Information for MNCs*. <https://www.china-briefing.com/news/china-cross-border-personal-information-transfer-new-clarifications-for-multinational-companies>.
- Huld, A. [Arense]. (28 March 2023). *China's Draft Certification Standards for Cross-Border Personal Information Transfer (Updated)*. <https://www.china-briefing.com/news/draft-certification-standards-for-cross-border-processing-of-personal-information>.
- Huld, A. [Arense]. (5 October 2022). *China Releases First Guidelines for Cross-Border Data Transfer Application*. <https://www.china-briefing.com/news/china-releases-first-guidelines-for-cross-border-data-transfer-application>.
- Huld, A. [Arense]. (6 June 2023). *Standard Contract Measures for Personal Information Export Come into Force June 1, Additional Guidelines Released*. <https://www.china-briefing.com/news/china-data-transfer-personal-information-export-standard-contract-procedures>.
- Hunton & Williams LLP. (2023). *35th International Conference of Data Protection and Privacy Commissioners*. https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/10/35th_Annual_International_Conference_of_Data_Protection_and_Privacy.pdf
- Hunton Williams. (2023). *United States Consumer Data Privacy Act of 2019*. <https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf>.
- ICC. (November 2033). *Privacy toolkit. An international business guide for policymakers*. <https://iccwbo.org/content/uploads/sites/3/2004/08/ICC-Privacy-Toolkit.pdf>.
- in 't Veld, Sophie. (26 January 2017). *Letter to EU Commission: What impact has Trump decisions on Privacy Shield and Umbrella Agreement?*. <https://www.sophieintveld.eu/letter-to-eu-commission-what-impact-has-trump-decisions-on-privacy-shield-and-umbrella-agreement>.
- Information Technology & Innovation Foundation. (2021). *Blocking the global flow of data*. <https://cdn.sanity.io/files/03hnmfyj/production/451f8f1ffcf72e97686f6bad3244706e7b8b7c6b.png>.
- International Association for Privacy Professionals. (25 July 2022). *Minister says India's Data Protection Bill 'a few months' away*. <https://iapp.org/news/a/minister-says-indias-data-protection-bill-a-few-months-away>.
- International Association of Privacy Professionals. (19 June 2023). *US State Privacy Legislation in 2022*. https://iapp.org/media/pdf/resource_center/infographic_privacy_matters_in_the_us_states.pdf.
- International Association of Privacy Professionals. (7 July 2023). *Comprehensive Consumer Privacy Bills*. https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.
- International Association of Privacy Professionals. (December 2021). *FTC Privacy Rulemaking*. https://iapp.org/media/pdf/resource_center/ftc_privacy_rulemaking_infographic.pdf.
- International Association of Privacy Professionals. (June 2023). *A practical comparison of the EU, China and ASEAN standard contractual clauses*. <https://iapp.org/resources/article/a-practical-comparison-of-the-eu-china-and-asean-standard-contractual-clauses/#sccs>.
- International Association of Privacy Professionals. (June 2023). *Global Privacy Law and DPA Directory*. <https://iapp.org/resources/global-privacy-directory>.
- International Association of Privacy Professionals. (May 2023). *Infographic: EU Data Initiatives in Context*. https://iapp.org/media/pdf/resource_center/recent_eu_data_initiatives_in_context_infographic.pdf.

- International Conference of Data Protection and Privacy Commissioners. (14 September 2004). *Resolution on a Draft ISO Privacy Framework Standard*. <https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-a-Draft-ISO-Privacy-Framework-Standard.pdf>.
- International Court of Justice. (9 July 2004). *Reports of judgments, advisory opinions and orders, Legal consequences of the construction of a wall in the occupied Palestinian territory*. <https://www.icj-cij.org/public/files/case-related/131/131-20040709-ADV-01-00-EN.pdf>.
- International Data Spaces Association. (April 2020). *Implementing the European Strategy on Data. Role of the International Data Spaces (IDS), Position Paper*. <https://internationaldataspaces.org/wp-content/uploads/IDSA-Position-Paper-Implementing-European-Data-Strategy-Role-of-IDS1.pdf>.
- International Monetary Fund (IMF). (October 2022). *World Economic Outlook Database*. <https://www.imf.org/en/Publications/WEO/weo-database/2022/October>.
- International Telecommunication Union. (12 December 2003). *Declaration of Principles, Building the Information Society: a global challenge in the new Millennium*. <https://www.itu.int/net/wsis/docs/geneva/official/dop.html>.
- Internet & Jurisdiction Policy Network. (2023). *Mission*. <https://www.internetjurisdiction.net/about/mission>.
- Internet & Jurisdiction Policy Network. (September 2020). *Infographic Internet Jurisdiction Policy Network September 2020*. <https://www.internetjurisdiction.net/uploads/pdfs/Infographic-Internet-Jurisdiction-Policy-Network-September-2020.pdf>
- Irion, K. [Kristina] and Yakovleva, S. [Svetlana] and Bartl, M. [Marija]. (13 July 2016). *Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements*. https://www.beuc.eu/publications/beuc-x-2016-070_trade_and_privacy-complicated_bedfellows_study.pdf.
- Irish Council for Civil Liberties. (15 April 2021). *New economic risk: draft US Senate Bill and Ireland's GDPR enforcement*. <https://www.iccl.ie/wp-content/uploads/2021/04/Letter.pdf>.
- Irish Council for Civil Liberties. (9 April 2021). *Economic & Reputational Risk of the DPC's Failure to Uphold EU Data Rights*. <https://www.iccl.ie/digital-data/economic-reputational-risk-of-the-dpcs-failure-to-uphold-eu-data-rights>.
- Irish Data Protection Commission. (15 March 2022). *Data Protection Commission announces decision in Meta (Facebook) inquiry*. <https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry>.
- Irish Data Protection Commission. (2 September 2021). *Data Protection Commission announces decision in WhatsApp inquiry*. <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>.
- Kabelka, L. [Laura]. (16 June 2022). *Sovereignty requirements remain in cloud certification scheme despite backlash*. <https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash>.
- Karr, T. [Timothy]. (11 March 2020). *Congress Tries to Sneak Through Dangerous Spying Bill Under the Cover of the Coronavirus Crisis*. <https://www.freepress.net/news/press-releases/congress-tries-sneak-through-dangerous-spying-bill-under-cover-coronavirus>.
- Kennedy, G. [Gabriela] and Woo, J. [Joshua]. (13 July 2022). *(Not So) Standard Contracts? Draft Standard Contracts Finally Released in China*. <https://www.mayerbrown.com/en/perspectives-events/publications/2022/07/not-so-standard-contracts-chinas-draft-standard-contractual-clauses-sccs-are-finally-released>.
- Kerry, C. F. [Cameron F.] and Morris, J. [John]. (19 June 2020). *Preemption: A balanced national approach to protecting all Americans' privacy*. <https://www.brookings.edu/blog/techtank/2020/06/29/preemption-a-balanced-national-approach-to-protecting-all-americans-privacy>.
- Kessler, F. [Florian] and Blöchl, J. [Jost]. (22 October 2018). *So wirkt Chinas Gesetz für Cybersecurity*. <https://www.divsi.de/so-wirkt-chinas-gesetz-fuer-cybersecurity/index.html>
- Kinsch, P. [Patrick]. (2009). *European Court of Human Rights (ECtHR)*. [https://max-eup2012.mpipriv.de/index.php/European_Court_of_Human_Rights_\(ECTHR\)](https://max-eup2012.mpipriv.de/index.php/European_Court_of_Human_Rights_(ECTHR)).
- Knoke, F. [Friederike] and Stoklas, J. [Jonathan]. *Internationales Forschungsprojekt zu elektronischen Beweisen in Strafverfahren*, ZD-Aktuell 2015, <https://beck-online.beck.de/Dokument?vpath=bibdata%5Czeits%5Czdaktuell%5C2015%5Ccont%5Czdaktuell.2015.04724.htm>.
- Konferenz der Justizministerinnen und Justizminister der Länder, Arbeitsgruppe "Digitaler Neustart". (15 May 2017). *Bericht vom 15. Mai 2017*. https://jm.rlp.de/fileadmin/mjv/Jumiko/Fruehjahrskonferenz_neu/Bericht_der_AG_Digitaler_Neustart_vom_15_Mai_2017.pdf.
- Kurzer, R. [Robin]. (13 August 2018). *The United States finally starts to talk about data privacy legislation*. <https://martechtoday.com/the-united-states-finally-starts-to-talk-about-data-privacy-legislation-219299>.
- Lai, K. [Karry]. (11 November 2021). *Primer: China's Data Security Law*. <https://www.iflr.com/article/b1vdly3c367qc/primer-chinas-data-security-law>.
- LaLonde, B. [Brandon]; Thompson, M. [Mark]; Kanthasamy, S. [Saz]. (2022). *IAPP-EY Annual Privacy Governance Report 2022 – Executive Summary*. <https://iapp.org/resources/article/privacy-governance-report/>.
- Lange / Filip, in: "BeckOK Datenschutzrecht", Wolff / Brink, 37th edition, 1 August 2020, Art. 49. Para. 8
- Legal Tribune Online. (29 January 2020). *Wir werden weitere Gutachten-Verfahren sehen*. <https://www.lto.de/recht/justiz/j/egmr-jahresbericht-statistik-2019-beschwerden-russland-tuerkei-gutachten-verfahren>.
- Leimbacher, J. [Jörg]. *Smart Regulation: Kurzfassung*. (2021). <https://www.aramis.admin.ch/Default?DocumentID=68333&Load=true>.

- Lelley, J.T. [Jan Tibor] and Yin, Y. [Yuanyuan]. (31 August 2021). *Cybersecurity & the New Data Security Law of the People's Republic of China*. <https://buse.de/en/insights/cybersecurity-the-new-data-security-law-of-the-peoples-republic-of-china>.
- Lienemann, G. [Georg]. (23 August 2021). *Parties to CoE Conventions 108 / 108+*. https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/lehrstuehle/hennemann/Mapping_Global_Data_Law/Sample_Convention_108.pdf
- Lomas, N. [Natasha]. (24 February 2022). *Privacy Shield 2.0 is high priority but not easy, warns EU's Vestager*. <https://techcrunch.com/2022/02/24/no-schrems-iii-pls>.
- Luo, Y. [Yan] and Yu, Z. [Zhijing] and Liu, V. [Vicky]. (22 June 2021). *The future of data localization and cross-border transfer in China: a unified framework or a patchwork of requirements?*. <https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements>.
- Max Planck Institute for Innovation and Competition. (1 August 2017). *Argumente gegen ein "Dateneigentum"*, 10 Fragen und Antworten. https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf.
- Max Planck Institute for Innovation and Competition. (23 March 2021). *Global Convergence of Data Protection Norms: Agenda for Trade and Development*. <https://www.ip.mpg.de/en/projects/details/global-convergence-of-data-protection-norms-agenda-for-trade-and-development.html>.
- Mayer, J. [Jonathan]. (3 December 2014). *Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier*. <http://webpolicy.org/2014/12/03/eo-12333-on-american-soil>.
- McKinsey Global Institute. (2016). *Digital globalization: The new era of global flows*. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>.
- Meta Inc. (17 August 2020). *Updating our international data transfer mechanisms*. <https://www.facebook.com/business/news/updates/our-international-data-transfer-mechanisms>.
- Moerel, L. [Lokke] and van der Wolk, A. [Alex]. (4 November 2021). *Why it is unlikely the announced supplemental SCCs will materialize*. <https://iapp.org/news/a/why-it-is-unlikely-the-announced-supplemental-sccs-will-materialize>.
- National Science Foundation. (2003). *A Brief History of NSF and the Internet*. https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.
- New America. *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china>.
- New York City Mayor's Office of the Chief Technology Officer. (2021). *IoT Strategy*. https://www1.nyc.gov/assets/cto/downloads/iot-strategy/nyc_iot_strategy.pdf.
- Nicodemus, A. [Aaron]. (5 May 2021). *Private right of action proving problematic for state privacy laws. Compliance Week*. <https://www.complianceweek.com/data-privacy/private-right-of-action-proving-problematic-for-state-privacy-laws/30343.article>.
- Ning, S. [Susan] and Han, W. [Wu] and Minlv, Y. [Yao] and Honglv, C. [Chen]. (17 December 2021). *Interpretation of the Measures on Security Assessment of Cross-border Data Transfer (Draft for Comment)*. <https://www.chinalawinsight.com/2021/12/articles/compliance/interpretation-of-the-measures-on-security-assessment-of-cross-border-data-transfer-draft-for-comment>.
- NOYB – European Center for Digital Rights. (7 October 2022). *New US Executive Order unlikely to satisfy EU Law*. <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>.
- NOYB – European Center for Digital Rights. (9 September 2020). *Is the DPC actually stopping Facebook's EU-US data transfers?! ...maybe half-way!*. <https://noyb.eu/en/dpc-actually-stopping-facebooks-eu-us-data-transfers-maybe-half-way>.
- NOYB – European Center for Digital Rights. (10 July 2023). *New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield". noyb will challenge the decision*. <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.
- NOYB – European Center for Digital Rights. (13 December 2022). *Statement on US Adequacy Decision by the European Commission*. <https://noyb.eu/en/statement-eu-commission-adequacy-decision-us>.
- NOYB – European Center for Digital Rights. (19 December 2019). *Generalanwalt unterstützt eine gezielten Lösung bei US-Massenüberwachung. Behörden müssen Datentransfers stoppen, wenn in USA Grundrechte nicht eingehalten werden. Ernsthafte Bedenken zu "Privacy Shield". Generalanwalt wendet EMRK statt GRC an. Schrems: "Gutachten folgt in praktisch allen Teilen unseren Argumenten"*. https://noyb.eu/sites/default/files/2020-03/pa_ag_19-12-2019_de.pdf.
- NOYB – European Center for Digital Rights. (25 March 2022). *Privacy Shield 2.0"? Erste Reaktion von Max Schrems*. <https://noyb.eu/de/privacy-shield-20-erste-reaktion-von-max-schrems>.
- NOYB – European Center for Digital Rights. (2022). *noyb's comments on the proposed Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679*. https://noyb.eu/sites/default/files/2020-12/Feedback_SCCs_nonEU.pdf.
- OneTrust. (7 March 2023). *International: CoE issues revised draft model contractual clauses*. <https://www.dataguidance.com/news/international-coe-issues-revised-draft-model>.
- Organization for Economic Co-operation and Development. (2018). *China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape*. <https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf>.

- Organization for Economic Co-operation and Development. (16 September 2014). *OECD computations based on Eurostat, Information Society Statistics and national sources*. <http://dx.doi.org/10.1787/888933148160>.
- Organization for Economic Co-operation and Development. (2019). *Implications of E-commerce for Competition Policy - Background Note*. [https://one.oecd.org/document/DAF/COMP\(2018\)3/en/pdf](https://one.oecd.org/document/DAF/COMP(2018)3/en/pdf).
- Organization for Economic Co-operation and Development. (2020). *Going Digital in Brazil, Chapter 6. Fostering the digital transformation of the Brazilian economy*. <https://www.oecd-ilibrary.org/sites/4f5ebe9d-en/index.html?itemId=/content/component/4f5ebe9d-en>.
- Organization for Economic Co-operation and Development. (2020). *Regulatory Impact Assessment*. <https://www.oecd.org/gov/regulatory-policy/regulatory-impact-assessment-7a9638cb-en.htm>.
- Organization for Economic Co-operation and Development. (2022). *Privacy Online: OECD Guidance on Policy and Practice, Part III, Inventory of Privacy-enhancing Technologies (PETs)*. <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/reg%282001%291/final>.
- Organization for Economic Co-operation and Development. (2022). *OECD Privacy Statement Generator*. <https://www.oecd.org/Internet/ieconomy/oecdprivacystatementgenerator.htm>.
- Organization for Economic Co-operation and Development. (2023). *Privacy*. <https://www.oecd.org/digital/ieconomy/privacy.htm>.
- Osborne Clark. (8 August 2022). *ADPPA vs GDPR*. <https://www.osborneclarke.com/system/files/documents/22/08/10/ADPPA%20vs%20GDPR.pdf>. P. 6.
- Patel, D. [Deepesh]. (2022). *Digital Ecosystems in Trade Finance: Seeing Beyond the Technology*. Trade Finance Global. <https://www.tradefinanceglobal.com/blockchain/digital-ecosystems-in-trade-finance/>.
- Piltz, C. [Carlo]. (7 Februar 2019). *Bundeskartellamt erlasst Untersagungsverfügung gegen Facebook – Warum das Vorgehen der Behörde datenschutzrechtlich kritisch betrachtet werden muss*. <https://www.delegedata.de/2019/02/bundeskartellamt-erlasst-untersagungsverfuegung-gegen-facebook-warum-das-vorgehen-der-behoerde-datenschutzrechtlich-kritisch-betrachtet-werden-muss/>
- Politico. (14 December 2020). *Inside the EU's divisions on how to go after Big Tech*. <https://www.politico.eu/article/margrethe-vestager-thierry-breton-europe-big-tech-regulation-digital-services-markets-act>.
- Potratz Metcalf, C. [Caitlin] and Lurie, A. [Adam] and Davison, D. [Doug]. (29 January 2020). *GDPR vs US Discovery: US Court Makes Clear Non-US Entities Can't Avoid Discovery*. <https://www.linklaters.com/en/insights/blogs/digilinks/2020/january/gdpr-vs-us-discovery>.
- Privacy and Civil Liberties Oversight Board. (10 February 2022). *Report and Recommendations on CIA Counterterrorism Activities Conducted Pursuant to E.O. 12333*. <https://www.pclob.gov/Oversight>.
- Privacy and Civil Liberties Oversight Board. (2020). *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*. https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%202011_19_20.pdf.
- Privacy International. (14 December 2022). *Recognition of Privacy in UN Human Rights Mechanisms*. <https://privacyinternational.org/privacy-un-human-rights-mechanisms>.
- Publications Office of the European Union. (2023). *Datasets*. <https://data.europa.eu/data/datasets?locale=en>.
- Rödl & Partner. (10 August 2022). *Outbound Data Transfer Security Assessment Measures*. <https://www.roedl.com/insights/cross-border-data-transfer-china-security-assessment-measures>.
- Rödl & Partner. (5 August 2020). *China's new Civil Code – Part 4: Personality Rights*. <https://www.roedl.com/insights/china-civil-code/part-4-personality-rights>.
- Rosenthal, D. [David]. (2022). *EU SCC Transfer Impact Assessment (TIA) Toolbox*. https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx.
- Sacks, S. [Samm]. (7 March 2019). *Testimony on "China: Challenges to U.S. Commerce, A Hearing Before the Senate Committee on Commerce, Science, and Transportation's, Subcommittee on Security*. <https://www.commerce.senate.gov/services/files/7109ED0E-7D00-4DDC-998E-B99B2D19449A>.
- Sait Akman, M. [Mehmet] et al. (7 October 2021). *Confronting Deglobalization in the Multilateral Trading System*. https://www.t20italy.org/wp-content/uploads/2021/09/TF3_PB02_LM04.pdf.
- Salvino, M. A. [Mary Ashley]. (1 November 2021). *Analysis: How Will the FTC Get Its Privacy Mojo Back*. <https://news.bloomberglaw.com/bloomberglaw-analysis/analysis-how-will-the-ftc-get-its-privacy-mojo-back-in-2022>.
- Sasso, B. [Brandan]. (12 June 2013). *NSA tracks phone locations under executive order*. <https://thehill.com/policy/technology/192294-nsa-uses-executive-order-to-track-phone-locations>.
- Schwartz, P. M. [Paul M.]. (2009). *Managing Global Data Privacy, Cross-Border Information Flows in a Networked Environment*. https://paulschwartz.net/wp-content/uploads/2019/01/Global_Data_Flows.pdf.
- Segal, B. [Ben]. (1995). *A Short History of Internet Protocols at CERN*. <https://ben.web.cern.ch/ben/TCPHIST.html>.
- Singh, M. [Manish]. (4 August 2022). *India withdraws personal data bill that alarmed tech giants*. <https://techcrunch.com/2022/08/03/india-government-to-withdraw-personal-data-protection-bill>.
- Sinolytics GmbH. (11 July 2022). *Adoption rate of international standards remains low in China*. https://sinolytics.de/sinolytics_weekly.
- Sinolytics GmbH. (11 July 2022). *China's cyber and data regulations: Maturing framework, increasing enforcement*. https://sinolytics.de/sinolytics_weekly.

- Sinolytics GmbH. (11 July 2022). *Digital economy: Important data and personal information enforcement takes center stage in next three years*. https://sinolytics.de/sinolytics_weekly.
- Spies, A. [Axel]. (September 2019). *US-District Court: Ist die DS-GVO ein Blockadegesetz (Blocking Statute)?*. <https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2019/us-district-court-is-the-gdpr-a-blocking-statute.pdf>.
- Stanford University. (18 August 2021). *Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)*. <https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021>.
- Statista GmbH. (13 September 2022). *Web analytics software market share worldwide 2022*. <https://www.statista.com/statistics/1258557/web-analytics-market-share-technology-worldwide>.
- Statista GmbH. (2020). *Industry 4.0 technologies expected to have the greatest impact on organizations worldwide as of 2020*. <https://www.statista.com/statistics/1200006/industry-40-technology-greatest-impact-organizations-worldwide>.
- Statista GmbH. (2021). *Datenvolumen des globalen IP-Traffics in den Jahren 2014 bis 2017 sowie eine Prognose bis 2022*. <https://de.statista.com/statistik/daten/studie/266869/umfrage/prognose-zum-datenvolumen-des-globalen-ip-traffics>.
- Statista GmbH. (2021). *Digital Economy Compass 2021*. <https://de.statista.com/statistik/studie/id/105648/dokument/digital-economy-compass/?locale=de>.
- Statista GmbH. (2023). *Digital Market Insights eCommerce*. <https://de.statista.com/outlook/dmo/ecommerce/weltweit>.
- Statista GmbH. (2023). *Meta dominiert die DSGVO-Top 10*. <https://de.statista.com/infografik/25449/fuer-verstoesse-gegen-datenschutzgesetze-verhaengte-geldbussen/>.
- Statista GmbH. (2023). *Ranking der größten Social Networks und Messenger nach der Anzahl der Nutzer im Januar 2023*. <https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user>.
- Statista GmbH. (2023). *Schätzung zur Anzahl der Internetnutzer weltweit für die Jahre 2005 bis 2022*. <https://de.statista.com/statistik/daten/studie/805920/umfrage/anzahl-der-internetnutzer-weltweit>.
- Statista GmbH. (2023). *Schätzung zur Anzahl der Internetnutzer weltweit nach Regionen im Juni 2022*. <https://de.statista.com/statistik/daten/studie/39490/umfrage/anzahl-der-internetnutzer-weltweit-nach-regionen>.
- Statista GmbH. (2023). *Werbeumsätze von Meta weltweit in den Jahren 2010 bis 2022*. <https://de.statista.com/statistik/daten/studie/458825/umfrage/werbeeinnahmen-von-facebook/?locale=de>.
- Statista GmbH. (24 January 2022). *Halten sich Internet-Dienste wie Google oder Facebook an die gesetzlichen Datenschutzbestimmungen oder halten sie sich nicht daran?*. <https://de.statista.com/statistik/daten/studie/827007/umfrage/umfrage-zum-umgang-mit-persoelichen-daten-durch-internet-dienste>.
- Statista GmbH. (31 May 2021). *Anzahl der anhängigen Verfahren am Europäischen Gerichtshof für Menschenrechte nach beklagten Ländern*. <https://de.statista.com/statistik/daten/studie/76450/umfrage/anhaengige-verfahren-am-europaeischen-gerichtshof-fuer-menschenrechte>.
- Statista GmbH. (5 May 2023). *Anteil der Befragten, die Bedenken haben, ihr privaten Daten bei amerikanischen Unternehmen zu speichern, in Deutschland in den Jahren 2010 bis 2018*. <https://de-statista-com.ezproxy.ip.mpg.de:8443/statistik/daten/studie/869457/umfrage/datenschutzbedenken-gegenueber-amerikanischen-anbietern-von-online-angeboten-in-deutschland>.
- Statista GmbH. (9 December 2021). *Anteil der Befragten, die sehr oder etwas besorgt über den Schutz ihrer Daten im Internet sind, in ausgewählten Ländern weltweit im Jahr 2018/19*. <https://de.statista.com/statistik/daten/studie/1021871/umfrage/bedenken-zum-datenschutz-im-internet-nach-laendern-weltweit>.
- Statista GmbH. (February 2019). *Forecast end-user spending on IoT solutions worldwide from 2017 to 2025*. <https://www.statista.com/statistics/976313/global-iot-market-size>.
- Svantesson, D. J. B. [Dan Jerker B.]. (22 January 2021). *How will China's new 'extraterritoriality shield' affect the Internet?*. <https://www.linkedin.com/pulse/how-chinas-new-extraterritoriality-shield-affect-svantesson/?trackingId=JDCdj1zwQISubFg616JUHA%3D%3D>.
- Swire, P. [Peter]. (18 July 2023). *A guide to the attorney general's finding of 'reciprocal' privacy protections in EU*. <https://iapp.org/news/a/a-guide-to-the-attorney-generals-finding-of-reciprocal-privacy-protections-in-eu/>.
- Teale, C. [Chris]. (12 January 2022). *More Than Half of Voters Back a National Data Privacy Law*. <https://morningconsult.com/2022/01/12/federal-data-privacy-legislation-polling>.
- The European Consumer Organization. (16 November 2020). *WTO trade talks must safeguard privacy, 42 organizations urge*. <https://www.beuc.eu/news/wto-trade-talks-must-safeguard-privacy-42-organisations-urge>.
- The Greens/EFA. (14 April 2016). *PNR air passenger data retention*. <https://www.greens-efa.eu/en/article/pnr-air-passenger-data-retention-6837>.
- The Lawfare Institute. (14 December 2020). *The Latest Skirmish in the Transatlantic Data Wars*. <https://www.lawfareblog.com/latest-skirmish-transatlantic-data-wars>.
- Thio, T.G. [Tse Gan]. (2018). *Data and privacy protection in ASEAN. – what does it mean for businesses in the region?*. <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf>.
- Tielemans, J. [Jetty]. (1 December 2021). *The EU's DMA and DSA: Why this should be of interest to privacy pros*. <https://iapp.org/news/a/developments-on-the-dma-and-dsa-why-this-should-be-of-interest-to-privacy-professionals>.

- Tomiura, E. [Eiichi] and Ito, B. [Banri] and Kang, B. [Byeongwoo]. (12 August 2020). *Regulating cross-border data flows: Firm-level analysis from Japan*. <https://voxeu.org/article/regulating-cross-border-data-flows>.
- Tomiura, E. [Eiichi] and Ito, B. [Banri] and Kang, B. [Byeongwoo]. (14 March 2020). *Cross-border data transfers under new regulations: Findings from a survey of Japanese firms*. <https://voxeu.org/article/cross-border-data-transfers-under-new-regulations>.
- United Kingdom, Information Commissioners' Office. (14 June 2022). *ICO funding update: Fine income retention agreement*. <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/ico-funding-update-fine-income-retention-agreement>.
- United Kingdom, Information Commissioners' Office. (7 March 2022). *National security and defense*. <https://ico.org.uk/for-organizations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/#work>.
- United Nations, Office of the High Commissioner for Human Rights. (2023). *Special Rapporteur on the right to privacy*. <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.
- United Nations, Office of the High Commissioner for Human Rights. (23 July 2023). *Human Rights Treaty Bodies - General Comments*. <https://www.ohchr.org/en/hrbodies/pages/tbgeneralcomments.aspx>.
- United Nations. (2023). *The 17 goals*. <https://sdgs.un.org/goals>.
- United Nations. (July 2021). *The UN System Chart*. https://www.un.org/en/pdfs/un_system_chart.pdf.
- United States of America, Chamber of Commerce. (17 June 2022). *Striking Similarities: Comparing Europe's Digital Markets Act to the American Innovation and Choice Online Act*. <https://www.uschamber.com/finance/antitrust/striking-similarities-dma-american-innovation-act>.
- United States of America, Chamber of Commerce. (31 May 2022). *U.S. Chamber Warns It Will Oppose Any Privacy Legislation That Creates a Blanket Private Right of Action*. <https://www.uschamber.com/technology/data-privacy/u-s-chamber-warns-it-will-oppose-any-privacy-legislation-that-creates-a-blanket-private-right-of-action>.
- United States of America, Department of Commerce. (12 April 2023). *Privacy Shield List*. <https://www.privacyshield.gov/list>.
- United States of America, Department of Justice. (28 December 2022). *Judicial Redress Act of 2015 & U.S.-EU Data Protection and Privacy Agreement*. <https://www.justice.gov/opcl/judicial-redress-act-2015>.
- United States of America, Federal Trade Commission. (2023). *Report Fraud to the FTC*. <https://reportfraud.ftc.gov/#/>.
- United States of America, Federal Trade Commission. (May 2021). *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*. <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>.
- United States of America, Office of Management and Budget. (2023). *Overview. Components of the Federal Data Strategy*. <https://strategy.data.gov/overview>.
- United States of America, Senate Committee on Commerce, Science, and Transportation. (3 June 2022). *House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill*. <https://www.commerce.senate.gov/2022/6/house-and-senate-leaders-release-bipartisan-discussion-draft-of-comprehensive-data-privacy-bill>.
- United States of America. *Gramm-Leach-Bliley Act*, 15 U.S.C. 6801-6809, (12 November 1999). ("GLBA").
- United States of America, Department of Commerce. (28 September 2020). *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*. <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>.
- United States of America, Department of Commerce. (September 2020). *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*. <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.pdf>.
- United States of America, Federal Communications Commission. (2023). *Privacy and Data Protection Task Force*. <https://www.fcc.gov/privacy-and-data-protection-task-force>.
- United States of America, Federal Trade Commission. (April 2013). *Children's Online Privacy Protection Rule: Not Just for Kids' Sites*. <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-not-just-kids-sites#who>.
- US-ASEAN Business Council. (2023). *Digital Data Governance in ASEAN*. https://www.usasean.org/system/files/downloads/digital_data_governance_in_asean-key_elements_for_a_data-driven_economy.pdf.
- Ustaran, E. [Eduardo]. (16 June 2022). *In search of a data localization strategy*. <https://www.linkedin.com/pulse/search-data-localization-strategy-eduardo-ustaran>.
- Veil, W. [Winfried]. (17 February 2018). *GDPR: 68 Obligations of the Controller*. <https://www.flickr.com/photos/winfried-veil/25437610017>.
- Voss, A. [Axel]. (25 May 2021). *Position Paper on Fixing the GDPR: Towards Version 2.0*. <https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf>.
- Web.de. (4 June 2018). *Fünf Jahre nach Snowden: Misstrauen gegenüber US-Anbietern auf Höchstwert*. *Repräsentative Kommunikationsstudie 2018, durchgeführt von Convios Consulting im Auftrag von GMX und WEB.DE*. https://www.slideshare.net/WEBDE_DEUTSCHLAND/fnf-jahre-nach-snowden-misstrauen-im-netz-auf-hchstniveau-100401931/1.
- Whittaker, Z. [Zack]. (28 June 2011). *Microsoft admits Patriot Act can access EU-based cloud data*. <https://www.zdnet.com/article/microsoft-admits-patriot-act-can-access-eu-based-cloud-data>.

- Wicker, R. [Roger]. (9 December 2020). *The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows*. U.S. Senate Committee on Commerce, Science, and Transportation. <https://www.commerce.senate.gov/2020/12/the-invalidation-of-the-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows#>.
- Wikileaks. (2023). *WikiLeaks Reveals Secret Files on All Guantánamo Prisoners*. <https://wikileaks.org/gitmo>.
- Wikipedia. (2023). *Structural evolution of the European Commission*. https://en.wikipedia.org/wiki/European_Communities.
- Wikipedia. (5 March 2023). *Supranational European Bodies*. https://en.wikipedia.org/wiki/File:Supranational_European_Bodies-en.svg.
- WilmerHale. (3 November 2021). *China Publishes Draft Measures on Security Assessment of Cross-Border Data Transfer*. <https://www.wilmerhale.com/en/insights/client-alerts/20201103-china-publishes-draft-measures-on-security-assessment-of-cross-border-data-transfer>.
- World Economic Forum. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf.
- World Trade Organization. (2022). *1.3 Definition of Services Trade and Modes of Supply*. https://www.wto.org/english/tratop_e/serv_e/cbt_course_e/c1s3p1_e.htm.
- World Trade Organization. (23 July 2023). *Members and Observers*. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.
- World Trade Organization. (4 April 2023). *Joint Initiative on E-commerce*. https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm.
- World Trade Organization. (December 2021). *WTO Joint Statement Initiative on E-commerce. Statement by Ministers of Australia, Japan and Singapore*. https://www.wto.org/english/news_e/news21_e/ji_ecom_minister_statement_e.pdf.
- Wu, E. [Emily]. (July 2021). *Sovereignty and Data Localization*. <https://www.belfercenter.org/publication/sovereignty-and-data-localization>.
- Wyden, R. [Ron]. (15 April 2021). *Wyden Releases Draft Legislation to Protect Americans' Personal Data From Hostile Foreign Governments*. <https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments>.
- Wyden, R. [Ron]. (2023). *The Protecting Americans' Data From Foreign Surveillance Act – Onepager*. <https://www.wyden.senate.gov/imo/media/doc/Protecting%20Americans%20Data%20from%20Foreign%20Surveillance%20Act%20of%202021%20One%20Pager.pdf>.
- Yang, S. [Samuel] and Fung, C. [Christopher] and Wu, L. [Leann]. (16 August 2022). *Will China's new certification rules be a popular legal path for outbound data transfers?*. <https://iapp.org/news/a/will-chinas-new-certification-rules-be-a-popular-legal-path-for-outbound-data-transfers>.
- Yangyang Su, P.C. [Peng Cai]. (12 November 2021). *China's Data Cross-border Rules are about to Fall into Place. Comments on the Measures for Security Assessment of Data Cross-border Transfer (Exposure Draft)*. http://www.zhonglun.com/Content/2021/11-12/1759271125.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.

12. Online newspapers, news reports

- Alper, A. [Alexandra] and Freifeld, K. [Karen]. (12 May 2022). Exclusive. Biden eyes new ways to bar China from scooping up U.S. data. *Reuters*. <https://www.reuters.com/world/us/exclusive-biden-eyes-new-ways-bar-china-scooping-up-us-data-2022-05-11>.
- Baraniuk, C. [Chris]. (24 October 2018). Tim Cook blasts 'weaponization' of personal data and praises GDPR. *BBC*. <https://www.bbc.com/news/technology-45963935>.
- Bartz, D. [Diane]. (28 May 2021). Biden seeks 11% jump in FTC funding as Big Tech cases loom. *Reuters*. <https://www.reuters.com/technology/biden-seeks-11-jump-ftc-funding-big-tech-cases-loom-2021-05-28>.
- Benner, K. [Katie] and Wee, S.-L. [Sui-Lee]. (4 January 2017). Apple Removes New York Times Apps From Its Store in China. *The New York Times*. <https://www.nytimes.com/2017/01/04/business/media/new-york-times-apps-apple-china.html>.
- Bodoni, S. [Stephanie]. (29 July 2022). Meta Repeats Why It May Be Forced to Pull Facebook From EU (1). *Bloomberg*. <https://news.bloomberglaw.com/privacy-and-data-security/meta-repeats-threat-it-may-pull-facebook-instagram-from-europe>.
- Bodoni, S. [Stephanie]. (30 July 2021). Amazon Gets Record USD 888 Million EU Fine Over Data Violations. *Bloomberg*. <https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach>.
- British Broadcasting Corporation. (30 October 2019). Facebook agrees to pay Cambridge Analytica fine to UK. *British Broadcasting Corporation*. <https://www.bbc.com/news/technology-50234141>.
- Chazan, G. [Guy]. (12 November 2019). Angela Merkel urges EU to seize control of data from US tech titans. *Financial Times*. <https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca>.
- Chee, F. Y. (Foo Yun). (2 June 2021). More safeguards in revamped EU data transfer tools, EU justice chief says. *Reuters*. <https://www.reuters.com/technology/more-safeguards-revamped-eu-data-transfer-tools-eu-justice-chief-says-2021-06-02>.

- Chee, F. Y. (Foo Yun). (4 December 2020). Not any time soon, says EU privacy watchdog. *Reuters*. <https://www.reuters.com/article/eu-privacy-idUSKBN28E2JQ>.
- Curi, M. [Maria]. (3 June 2022). Bipartisan Draft Bill Would Fortify Children's Data Privacy (3). *Bloomberg*. <https://about.bgov.com/news/bipartisan-draft-bill-would-fortify-childrens-data-privacy-2>.
- Curi, M. [Maria]. (13 July 2022). California Democrats Demand Stronger Privacy Protection Bill (2). *Bloomberg*. <https://news.bloomberglaw.com/privacy-and-data-security/california-democrats-push-for-stronger-privacy-protection-bill>
- de Carbonnel, A. [Alissa]. (6 April 2018). EU says Facebook confirmed data of 2.7 million Europeans 'improperly shared'. *Reuters*. <https://www.reuters.com/article/us-facebook-cambridge-analytica-eu-lette-idUSKCN1HD1AJ>
- dpa Deutsche Presse Agentur GmbH. (12 March 2016). Merkel: Daten sind die Rohstoffe des 21. Jahrhunderts. *Frankfurter Allgemeine Zeitung*. <https://www.faz.net/aktuell/wirtschaft/cebitt/angela-merkel-fordert-mehr-modernisierte-digitale-technologien-14120493.html>.
- dpa Deutsche Presse Agentur GmbH. (19 January 2010). Illegale Überwachung: FBI erschlich sich Telefondaten zur Terrorabwehr. *Der Spiegel*. <http://www.spiegel.de/politik/ausland/illegale-ueberwachung-fbi-erschlich-sich-telefondaten-zur-terrorabwehr-a-672646.html>.
- European Commission. (9 March 2021). Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030. *European Parliamentary Research Service*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983.
- Fioretti, J. [Julia] and Volz, D. [Dustin]. (26 October 2016). Privacy group launches legal challenge against EU-U.S. data pact. *Reuters*. <https://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK>.
- Frankfurter Allgemeine Zeitung*. (17 July 2023). KI-Sicherheitslabel im Gespräch. P. 17.
- Frankfurter Allgemeine Zeitung*. (20 July 2013). Merkel regt globales Datenschutz-Abkommen an. www.faz.net/aktuell/politik/spaehaffaere-merkel-regt-globales-datenschutz-abkommen-an-12288963.html
- Gathmann, F. [Florian]. (10 August 2010). Google überrumpelt urlaubende Ministerinnen. *Der Spiegel*. <https://www.spiegel.de/politik/deutschland/street-view-start-google-ueberrumpelt-urlaubende-ministerinnen-a-711073.html>.
- Gellman, B. [Barton] and Poitras, L. [Laura]. (7 June 2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
- Gellman, B. [Barton] and Soltani, A. [Ashkan]. (4 December 2013). NSA tracking cellphone locations worldwide, Snowden documents show. *The Washington Post*. https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.
- Goujard, C. [Clothilde]. (31 March 2023). Italian privacy regulator bans ChatGPT. *Politico*. <https://www.politico.eu/article/italian-privacy-regulator-bans-chatgpt>.
- Greenwald, G. [Glenn] and MacAskill, E. [Ewan]. (11 June 2013). Boundless Informant: the NSA's secret tool to track global surveillance data. *The Guardian*. <https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>.
- Hänel, L. [Lisa]. (2 May 2029). Zensur im Netz: Russland folgt Chinas Beispiel. *Deutsche Welle*. <https://www.dw.com/de/zensur-im-internet-nimmt-zu-russland-folgt-chinas-beispiel/a-48575267>.
- Horwitz, J. [Jeff]. (15 June 2018). AP: Trump 2020 working with ex-Cambridge Analytica staffers. *Associated Press*. <https://apnews.com/article/north-america-technology-ap-top-news-elections-donald-trump-96928216bdc341ada659447973a688e4>.
- Horwitz, J. [Josh]. (30 September 2021). China drafts new data measures, defines "core data". *Reuters*. <https://www.reuters.com/world/china/china-issues-draft-rule-data-security-industry-telecoms-2021-09-30>.
- Julia Fioretti, J. [Julia]. (26 February 2018). Europe seeks power to seize overseas data in challenge to tech giants. *Reuters*. <https://www.reuters.com/article/uk-eu-data-order-idUKKCN1GA0LN>.
- Kern, R. [Rebecca]. (1 June 2022). Lawmakers reach bipartisan compromise on privacy bill with preemption, right to sue. *Politico*. <https://subscriber.politicopro.com/article/2022/06/lawmakers-reach-bipartisan-compromise-on-privacy-bill-with-preemption-right-to-sue-00036563?source=email>.
- Kirkpatrick, M. [Marshall]. (10 January 2021). Facebook's Zuckerberg Says The Age of Privacy Is Over. *The New York Times*. <https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html>.
- Klosowski, T. [Thorin]. (6 September 2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *The New York Times*. <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us>.
- Köcher, R. [Renate]. (27 July 2023). Diffuse Ängste. *Frankfurter Allgemeine Zeitung*.
- Leutheusser-Schnarrenberger, S. [Sabine] et al. (27 October 2011). Wir sollten nach der Ohrfeige einen Schritt zurücktreten. *Frankfurter Allgemeine Zeitung*. <https://www.faz.net/aktuell/feuilleton/debatten/staatstrojaner/sabine-leutheusser-schnarrenberger-im-gespraech-wir-sollten-nach-der-ohrfeige-einen-schritt-zuruecktreten-11508374.html>.
- Lima, C. [Cristiano]. (16 September 2021). Why Democrats are rallying around creating a new FTC privacy bureau to police Big Tech. *The Washington Post*. <https://www.washingtonpost.com/politics/2021/09/16/why-democrats-are-rallying-around-creating-new-ftc-privacy-bureau-police-big-tech>.

- Lu, S. [Shen]. (10 December 2020). Facial Recognition Is Running Amok in China. The People Are Pushing Back. *VICE*. <https://www.vice.com/en/article/4adnyq/facial-recognition-is-running-amok-in-china-the-people-are-pushing-back>.
- MacAskill, E. [Ewan] and Borger, J. [Julian] and Hopkins, N. [Nick]. (21 June 2013). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*. <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.
- Madiega, T. [Tambiama]. (January 2022). Artificial intelligence act. *European Parliamentary Research Service*. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf).
- Manancourt, V. [Vincent] and Scott, M. [Mark]. (25 March 2022). Political pressure wins out as US secures preliminary EU data deal. *Politico*. <https://www.politico.eu/article/privacy-shield-data-deal-joe-biden-ursula-von-der-leyen>.
- Manancourt, V. [Vincent] and Scott, M. [Mark]. (31 March 2022). The West's plan to keep global data flows alive. *Politico*. <https://www.politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/data-oecd-privacy-shield-national-security/amp>.
- Manancourt, V. [Vincent]. (2 December 2021). Top EU official warns privacy rules may need to change. *Politico*. <https://www.politico.eu/article/eu-privacy-regulators-clash-gdpr-enforcement>.
- Manancourt, V. [Vincent]. (22 August 2022). Norway wants Facebook fined for illegal data transfers. *Politico*. <https://www.politico.eu/article/norway-wants-facebook-to-be-fined-for-illegal-data-transfers>.
- Manancourt, V. [Vincent]. (25 March 2022). EU, US strike preliminary deal to unlock transatlantic data flows. *Politico*. <https://www.politico.eu/article/eu-us-strike-preliminary-deal-to-unlock-transatlantic-data-flows>.
- Manancourt, V. [Vincent]. (5 September 2022). Instagram fined EUR 405M for violating kids' privacy. *Politico*. <https://www.politico.eu/article/instagram-fined-e405m-for-violating-kids-privacy>.
- Manancourt, V. [Vincent]. (7 July 2022). Europe faces Facebook blackout. *Politico*. <https://www.politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/europe-faces-facebook-blackout-instagram-meta-data-protection/amp>.
- Meller, P. [Paul]. (22 September 2003). Europe Fights U.S. Over Passenger Data. *The New York Times*. <http://www.nytimes.com/2003/09/22/business/worldbusiness/22FLY.html?pagewanted=1>.
- Mohr, D. [Daniel]. (6 July 2023). KI besser als MSCI-World-ETF. *Frankfurter Allgemeine Zeitung*. P. 27.
- Mozur, P. [Paul]. (20 July 2017). Beijing Wants A.I. to Be Made in China by 2030. *The New York Times*. <https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html>.
- Nicodemus, A. [Aaron]. (5 May 2021). Private right of action proving problematic for state privacy laws. *Compliance Week*. <https://www.complianceweek.com/data-privacy/private-right-of-action-proving-problematic-for-state-privacy-laws/30343.article>.
- Peteranderl, S. [Sonja]. (11 June 2019). Alle Daten an alle Staaten. *Der Spiegel*. <https://www.spiegel.de/netzwelt/netzpolitik/e-evidence-warum-die-eu-plaene-zu-digitalen-beweisen-gefaehrlich-sind-a-1270939.html>.
- Rappeport, A. [Alan]. (17 September 2019). U.S. Outlines Plans to Scrutinize Chinese and Other Foreign Investment. *The New York Times*. <https://www.nytimes.com/2019/09/17/us/politics/china-foreign-investment-cfius.html>.
- Reißmann, O. [Ole]. (10 March 2011). Privatsphäre ist so was von Eighties. *Der Spiegel*. <https://www.spiegel.de/netzwelt/netzpolitik/internet-exhibitionisten-spackeria-privatsphaere-ist-sowas-von-eighties-a-749831.html>.
- Reuters*. (23 September 2021). ACLU, 26 other groups support USD 1 billion boost for FTC privacy work. <https://www.reuters.com/world/us/aclu-26-other-groups-support-1-billion-boost-ftc-privacy-work-2021-09-23>.
- Reuters*. (15 September 2021). U.S. panel votes to approve USD 1 billion for FTC privacy probes. <https://www.reuters.com/business/us-panel-votes-approve-1-billion-ftc-privacy-probes-2021-09-14>.
- Romm, T. [Tony]. (27 July 2018). The Trump administration is talking to Facebook and Google about potential rules for online privacy. *The Washington Post*. <https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy>.
- Rosenberg, M. [Matthew] and Confessore, N. [Nicholas] and Cadwalladr, C. [Carole]. (17 March 2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.
- Satariano, A. [Adam]. (22 May 2023). Meta Fined \$1.3 Billion for Violating E.U. Data Privacy Rules. *The New York Times*. <https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>.
- Scott, M. [Mark]. (13 January 2022). Digital Bridge: US lawmaking stalled – Europe's (other) digital rules – France's Cédric O". *Politico*. <https://www.politico.eu/newsletter/digital-bridge/us-lawmaking-stalled-europes-other-digital-rules-frances-cedric-o>.
- Scott, M. [Mark]. (2 June 2021). Biden seeks high-level data deal to repair EU-US digital ties. *Reuters*. <https://www.politico.eu/article/joe-biden-data-transfers-privacy-shield-eu-transatlantic>.
- Scott, M. [Mark]. (3 February 2022). Digital Bridge: Privacy Shield update 3.0 — Semiconductor subsidies — EU-US policy spat. *Politico*. <https://www.politico.eu/newsletter/digital-bridge/privacy-shield-update-3-0-semiconductor-subsidies-eu-us-policy-spat>.
- Shane, S. [Scott]. (9 June 2011). Ex-N.S.A. Aide Gains Plea Deal in Leak Case; Setback to U.S. *The New York Times*. https://www.nytimes.com/2011/06/10/us/10leak.html?_r=2&pagewanted=1&hp.
- Shepardson, D. [David]. (27 July 2018). Trump administration working on consumer data privacy policy. *Reuters*. <https://www.reuters.com/article/us-usa-internet-privacy-idINKBN1KH2MK>.

- Smout, A. [Alistair]. (30 October 2019). Facebook agrees to pay UK fine over Cambridge Analytica scandal. *Reuters*. <https://www.reuters.com/article/us-facebook-privacy-britain-idCAKBN1X9130>.
- Stölzel, T. [Thomas]. (10 August 2011). Amerika liest mit. *WirtschaftsWoche*. <https://www.wiwo.de/technologie/spionage-amerika-liest-mit-5317814.html>.
- Stupp, C. [Catherine]. (9 September 2022). *G-7 Privacy Regulators Aim To Ease Turbulent International Data Flows*. The Wall Street Journal. <https://www.wsj.com/articles/g-7-privacy-regulators-aim-to-ease-turbulent-international-data-flows-11662730512>.
- Wissing, V. [Volker]. (15 July 2023). KI braucht innovative Regulierung. *Frankfurter Allgemeine Zeitung*. P. 23.
- Ye, J. [Josh]. (23 January 2017). China tightens Great Firewall by declaring unauthorized VPN services illegal. *South China Morning Post*. <https://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall>.
- Zhong, R. [Raymond]. (1 September 2021). China fines Alibaba USD 2.8 Billion in Landmark Antitrust Case. *The New York Times*. <https://www.nytimes.com/2021/04/09/technology/china-alibaba-monopoly-fine.html>.
- Zuckerberg, M. [Mark]. (30 March 2019). Opinion: Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas. *The Washington Post*. https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

13. Conference sessions

- Barayre, C. [Cécile]. (5 July 2016). *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. MIKTA Workshop on Electronic Commerce, Geneva, Switzerland. https://www.wto.org/english/forums_e/business_e/3_4_Cecile_ppt.pdf.
- Gencarelli, Bruno. (20 July 2023). *EU data transfers: The latest and what comes next*. <https://www.linkedin.com/events/7086781491065577472>.
- Georgescu, F. [Florin]. (18 November 2021). *PrivacyConnect*. Zurich. <https://event.on24.com/wcc/r/3380148/72924565275FB73E289A885729C0DF08?mode=login&email=philipp.fischer@ip.mpg.de>.
- Greenstein, A. [Alex]. (14 July 2023). *The EU-U.S. Data Privacy Framework in practice*. <https://www.linkedin.com/events/theeu-u-s-dataprivacyframeworki7084583977969164288>.
- Heather, S. [Sean]. (28 February 2022). *Hope Springs Eternal? Assessing the State of U.S.-EU Digital Cooperation*. State of the Net conference in Washington, D.C. <https://www.stateofthenet.org/sotn-22>.
- Hörmler, J. [Julia]. (26 March 2021). *Roundtable - Overcoming the Jurisdictional Challenge of the Internet?*. Queen Mary University of London, Centre for Commercial Law Studies. <https://www.qmul.ac.uk/ccsl/events/past-events/videos-and-recordings/overcoming-jurisdictional-challenge-of-internet>.
- International Association of Privacy Professionals. (29 April 2021). *Keynote: EU-U.S. Data Transfers: The Road Ahead*. <https://www.linkedin.com/video/live/urn:li:ugcPost:6793534522072801280/?isInternal=true>
- Lopez Gonzalez, J. [Javier]. (9 November 2020). *Trade and cross-border data flows. Mapping the policy environment and thinking about the economic implications*. WTO Trade Dialogues. https://www.wto.org/english/res_e/reser_e/2_javier_lopez_gonzales_wto_dialogues_november_2020_rev3.pdf.

14. Photograph, print or poster

- Kulhari, S. [Shradha]. (2023). *Global Convergence of Data Protection Norms: An Agenda for Development & Trade*. Poster, Max Planck Institute for Innovation and Competition, Munich.

15. Podcast

- Dausend, P. [Peter] and Hildebrandt, T. [Tina]. (8 July 2022). Der Krieg ist klimapolitisch ein Desaster. In *Das Politikteil / Energiewende*. Zeit Online. https://www.zeit.de/politik/2022-07/energiewende-energiepolitik-ukraine-krieg-politikpodcast?utm_referrer=https%3A%2F%2Fwww.google.com%2F.

16. Tweet

- Van der Leyen, U. [Ursula]. @vonderleyen. (25 March 2022). *Pleased that we found an agreement in principle on a new framework for transatlantic data flows. It will enable predictable and trustworthy EU-US data flows, balancing security, the right to privacy and data protection. This is another step in strengthening our partnership*. <https://twitter.com/vonderleyen/status/1507286853224914949>.

17. Videos

- Carroll, D. [David]. (24 July 2019). *The Great Hack*. Netflix. <https://www.netflix.com/watch/80117542?source=35>.

- Jónsdóttir, B. [Birgitta]. (8 May 2016). *Being offline is the new luxury*. Netherlands Public Broadcasting (NPO), VPRO Documentary. <https://www.vpro.nl/programmas/tegenlicht/kijk/backlight/Offline-is-the-new-luxury.html>.
- Kaiser, B. [Brittany]. (24 July 2019). *The Great Hack*. Netflix. <https://www.netflix.com/watch/80117542?source=35>.
- Kirk, M. [Michael] et al. (13 May 2014). *United States of Secrets*. WGBH Educational Foundation. <https://www.pbs.org/wgbh/frontline/documentary/united-states-of-secrets>.
- The Daily Show. (20 September 2019). *Interview with Edward Snowden. Edward Snowden - Permanent Record & Life as an Exiled NSA Whistleblower*. <https://www.youtube.com/watch?v=PArFP7ZJrtg>.
- von der Leyen, U. [Ursula]. [European Commission]. (2 June 2021). *Message by President von der Leyen - "Leading the Digital Decade"*. YouTube. <https://www.youtube.com/watch?v=kpTDZMqkzxl>.
- WGBH Educational Foundation, Frontline Documentary. (5 November 2019). *In the age of AI*. YouTube. <https://www.youtube.com/watch?v=tyGEejOBdFc>.