UNIVERSITY OF TRENTO - Italy

School of International Studies

University of Trento
Doctoral Programme in International Studies

Exchanging and Protecting Personal Data across Borders:

GDPR Restrictions on International Data Transfer

by

Isabella Oldani

Thesis submitted in partial fulfilment of the requirements for the degree of
Doctor of Philosophy in International Studies

Supervisor: Prof. Antonino Alì

8th July 2020

Abstract

From the very outset of the EU data protection legislation, and hence from the 1995 Directive, international data transfer has been subject to strict requirements aimed at ensuring that protection travels with data. Although these rules have been widely criticized for their inability to deal with the complexity of modern international transactions, the GDPR has essentially inherited the same architecture of the Directive together with its structural limitations.

This research aims to highlight the main weaknesses of the EU data export restrictions and identify what steps should be taken to enable a free, yet safe, data flow. This research first places EU data transfer rules in the broader debate about the challenges that the un-territorial cyberspace poses to States' capabilities to exert their control over data. It then delves into the territorial scope of the GDPR to understand how far it goes in protecting data beyond the EU borders. The objectives underpinning data export restrictions (i.e., avoiding the circumvention of EU standards and protecting data from foreign public authorities) and their limitations in achieving such objectives are then identified.

Lastly, three possible "solutions" for enabling data flow are tested. Firstly, it is shown that the adoption by an increasing number of non-EEA countries of GDPR-like laws and the implementation by many companies of GDPR-compliant policies is more likely to boost international data flow than internationally agreed standards. Secondly, the role that Article 3 GDPR may play in making data transfer rules "superfluous" is analysed, as well as the need to complement the direct applicability of the GDPR with cross-border cooperation between EU and non-EU regulators. Thirdly, the study finds that the principle of accountability, as an instrument of data governance, may boost international data flow by pushing most of the burden for ensuring GDPR compliance *on* organizations and *away* from resource-constrained regulators.

Acknowledgments

I would like to thank the School of International Studies for having given me the opportunity to start this journey. These three years have given me the time and the resources for delving into what I find an extremely interesting subject.

I thank my supervisor, Professor Antonino Alì, for his support and advice. I also would like to thank Mark Beittel for his encouraging words, and for teaching me how to express in simple terms my complex thoughts.

I am deeply grateful to the Cloud Legal Project for having me as a visiting research student and for making me feel part of the team. The daily discussions with the members of the team have not only helped me increase my understanding of the subject but also discover my professional path.

I also would like to thank all the wonderful friends that I have made along this journey. A special thank goes to my PhD colleagues with which I have shared some of the happiest and toughest moments over the past three years.

Thanks to my family for their unconditional support and to my boyfriend for his patience and for his faith in my abilities.

Table of Contents

Abbreviations

A29WP	Article 29 Working Party
AA	Administrative Arrangement pursuant to Article 46(3)(b) GDPR
APEC	Asia-Pacific Economic Cooperation
BCRs	Binding Corporate Rules
BRICS	Brazil, Russia, India, China and South Africa
CBPR	APEC Cross-Border Privacy Rules
CCPA	California Consumer Privacy Act
CILP	Centre for Information Policy Leadership
Cloud Act	US Clarifying Lawful Overseas Use of Data Act
CPEA	Cross-border Privacy Enforcement Arrangement (APEC)
CSPs	Communications Services Providers
DP Agreement	Data Processing Agreement
DPA	Data Protection Authority
DPD (or 1995 Directive)	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
DPO	Data Protection Officer
ECIPE	European Centre for International Political Economy
ECJ	European Court of Justice
ECSG	APEC Electronic Commerce Steering Group
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EEC Treaty	Treaty establishing the European Economic Community
EU	European Union

FISA	US Foreign Intelligence Surveillance Act
FRA	European Union Agency for Fundamental Rights
GDPR (or Regulation)	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 (General Data Protection Regulation)
GPS	Global Positioning System
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil & Political Rights
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICO	Information Commissioner's Office
ILC	International Law Commission
IP address	Internet Protocol address
LGPD	Lei Geral e Única de Proteção de Dados Pessoais (Brazil)
LIBE Committee	European Parliament Committee on Civil Liberties, Justice and Home Affairs
MLA(T)	Mutual Legal Assistance (Treaty)
NSA	US National Security Agency
OECD	Organisation for Economic Cooperation and Development
OPC	Office of the Privacy Commissioner of Canada
PEA	Privacy Enforcement Authority (APEC)
PIMFA	Personal Investment Management & Financial Advice Association
PIPEDA	Canadian Personal Information Protection and Electronic Documents Act
PPC	Personal Information Protection Commission (Japan)
PRP	APEC Privacy Recognition for Processor
SCA	US Stored Communications Act
SCCs	Standard Contractual Clauses

SME	Small and Medium Sized Enterprise
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TiSA	Trade in Services Agreement
TTIP	Transatlantic Trade and Investment Partnership
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
WGIEC	Working Group on International Enforcement Cooperation (ICDPPC)
WTO	World Trade Organization

Index of Tables

1. Introduction

Everyone could guess, and is probably aware, that when we book an hotel in Japan or when we purchase our clothes online from our favourite US brand, our data move across border. However, fewer people may know that international data transfer is also triggered in some other less "obvious" situations, for example, when we upload our documents on Dropbox,[1] when we search for a book on Amazon,[2] when we open a Gmail account[3] or sign up to an event on Eventbrite.[4] In all these scenarios, our data may be transferred to servers or third parties which are located outside the country where we live, outside the European Union (EU), and outside the European Economic Area (EEA). Data transfer also occurs when data are located in the European Union but are accessed remotely by a company in a non-EU country or when, in offering a specific product, a company in the EU outsources some of the processing activities to another company outside the EU. In this framework, occasional data transfers between identified individuals have been replaced by "a continuous, multipoint global data flow"[5] where a number of different agents may be involved either transferring data for their own purposes or on behalf of other parties. Moreover, this data flow is no longer nurtured mainly by business-business relationships, but individuals have also started to play an active role in generating this flow (albeit often unknowingly) by conducting their daily online activities.[6] Personal data can be emailed, messaged, tweeted, accessed, copied and backed up with the click of a mouse in multiple, sometimes unpredictable, locations across the globe.[7]

---

[1] Dropbox Privacy Policy, last modified December 17, 2019, accessed December 29, 2019, https://www.dropbox.com/privacy.

[2] Amazon Privacy Notice, last modified September 23, 2019, accessed December 29, 2019, https://www.amazon.co.uk/gp/help/customer/display.html?ie=UTF8&nodeId=201909010&ref_=footer_privacy#GUID-A440AA65-7F7E-4134-8FA8-842156F43EEE__SECTION_22160257376047E78334D565CD73852D.

[3] Google Privacy Policy, last modified October 15, 2019, accessed December 29, 2019, https://policies.google.com/privacy?gl=IT&hl=en-GB.

[4] Eventbrite Privacy Policy, last modified December 16, 2019, accessed December 29, 2019, https://www.eventbrite.com/support/articles/en_US/Troubleshooting/eventbrite-privacy-policy?lg=en_US

[5] Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 2013, 151, accessed May 22, 2019, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[6] Ibid., 85–86.

[7] W. Kuan Hon and Christopher Millard, "How Do Restrictions on International Data Transfers Work in Clouds?," in *Cloud Computing Law* (Oxford: Oxford University Press, 2013), 275.

Data flow has grown more *global*, meaning that sellers and buyers in opposite parts of the world can easily connect "with a few clicks"; more *inclusive*, meaning that global trade is no longer in the hands of a few multinational companies, but it also hosts "millions of small enterprises";[8] and *indispensable* to the growth and the well-functioning of global economy of which data are the raw material. "Cross-border flows of personal data occur for any number of reasons: e-commerce, e-government, online banking, human resources management, distance education, online gambling, community activities or health research – to name a few areas".[9] This evolution has certainly increased organizations' efficiency and user convenience. Organizations can offer their services to their customers at a distance while allowing their customers to easily bridge this distance by means of an Internet connection. Greater flexibility, lower costs and more mobility that derive from the use of new technologies benefit both multinational and small and medium-sized organizations as well as individuals.[10]

While data location seems to have lost its relevance in a context where data are routinely transferred across different jurisdictional borders, it has certainly retained a great deal of importance at the national, regional, but also international levels where data location is still perceived as a source of concerns. Depending on the degree (and the nature) of these concerns, countries have adopted different rules regulating and controlling the movement of data from, to and through their borders. In the European Union, data transfer rules are an essential component of the data protection framework. Indeed, from the very outset of the EU data protection legislation, and hence from the adoption of the 1995 Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995 Directive or DPD)[11] – which was built on the premises of the

[8] Jacques Bughin and Susan Lund, "The Ascendancy of International Data Flows," *McKinsey Global Institute*, January 9, 2017, accessed December 29, 2019, https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows.

[9] Organisation for Economic Cooperation and Development, *Report on the Cross-Border Enforcement of Privacy Laws*, 2006, 7, accessed April 14, 2019, http://www.oecd.org/internet/ieconomy/37558845.pdf.

[10] Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 86–87.

[11] European Parliament and Council of the 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* (OJ L 281/31, 1995).

OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)[12] and of the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[13] – the transfer of personal data from the EU to third countries (i.e., non-EEA countries) has been subject to strict requirements. As it will be further discussed in the course of this dissertation (chapter 4), such requirements are meant to avoid the circumvention of the EU data protection standards once data are transferred to jurisdictions with lower standards of protection. Since then, the DPD has been recognized internationally as the instrument that lays out the strongest standards for data protection[14] and its rules on transborder data flow have become a benchmark for cross-border data flow in other jurisdictions.[15]

At the same time, data transfer rules have been widely criticized and the need for a reform have been voiced by many parties. Indeed, such rules seem to be unfit for coping with the relentless movement of data across borders and with the complexity of modern international transactions. In other words, these provisions are of limited utility when, instead of flowing from one point straight to another, data are transferred by and among multiple parties in multiple locations. The complexity of modern data flow and the development of new technologies such as cloud computing was probably not foreseen when the 1995 Directive has been drafted: the "Directive's framework for international transfers was designed for a different era. Over the past years, the Internet has radically redefined the way we communicate, access content, and share information, ushering in a new era of 'online' or 'cloud' computing".[16] Moreover, provisions on international data transfer often translate into purely

[12] Organisation for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (C(80)58/FINAL, 1980), (hereafter cited as 1980 OECD Guidelines).

[13] Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Strasbourg: ETS No.108, 1981), (hereafter cited as Convention 108).

[14] Dan Jerker B. Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," *Stanford Journal of International Law* 50, no. 1 (2014): 62–63.

[15] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, COM(2017) 7 final. (Brussels, 2017), 4, accessed April 15, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

[16] Microsoft Corporation, *Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009, 4, accessed August 6, 2018, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/microsoft_corporation_en.pdf.

formal requirements with a limited capacity of increasing users' privacy. The implementation of these rules often requires companies to undertake time-consuming and expensive activities which, however, have a limited chance of enhancing users' protection. Simply put, data transfer rules prescribed under the 1995 Directive seem to focus more on detailed and prescriptive requirements rather than on substantive outcomes.[17] To describe this mismatch between prescriptive provisions and substantive outcomes, Hon (2018) has called data transfer rules as a "Frankenrule": just like Frankenstein created a creature who took life on its own, compliance with data transfer rules seem to be pursued independently of compliance with the substantive data protection principles that such rules are meant to enforce.[18]

Moreover, data transfer rules set out under the 1995 Directive have been not only widely criticized but also largely disregarded by companies. Even if gathering direct evidence on non-compliance is hard, non-compliance emerges from some indirect evidence: since the volume of data transfers is high and many of those transfers must be conducted otherwise than by implementing data transfer rules, many of those transfers must be non-compliant.[19] The fact that many large economies, like China, are not among the countries that have been "whitelisted" by the European Commission also suggests that most of the transfers to those economies must be non-compliant.[20] Non-compliance may derive from lack of awareness on the part of the companies exporting data. In other words, just like users may not be aware of the data transfers they "trigger" (unless they read carefully the privacy policies of the services they use), businesses handling their customers' data might be unaware of the legal obligations stemming from these transfers. Another possibility is that, even assuming that companies exporting data are aware of their obligations, they might deliberately choose not to comply

[17] Ibid., 5.

[18] W. Kuan Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens* (Cheltenham, UK: Edward Elgar Publishing, 2017), 1.

[19] Ibid., 226.

[20] Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future* (TILT Law & Technology Working Paper No. 016/2010 - Tilburg Law School Research Paper No. 016/2010, 2010), 29, accessed February 9, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483.

with data transfer rules in order to avoid costs and delays.[21] Despite this high level of non-compliance, very little enforcement actions have been taken by national Data Protection Authorities (DPAs). This is probably due to the lack of resources or the lack of the technical abilities to monitor the huge volume of daily data transfers and hence to detect non-compliance.[22] The weakness of the enforcement actions taken by DPAs have been acknowledged by the European Commission back in 2003 when it noted that "many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection. Yet there is little or no sign of enforcement actions by the supervisory authorities".[23]

Despite these criticisms, the General Data Protection Regulation (GDPR or Regulation),[24] which became directly applicable as of 25 May 2018 and repealed the previous Directive, has essentially inherited the same architecture of the 1995 Directive. As it will be discussed in greater detail in chapter 5, the administrative simplifications and the new legal bases for transfer that have been introduced by the GDPR seem insufficient to counterbalance the weaknesses and the limitations of the data transfer framework. In other words, if one of the main scopes of the GDPR was to modernize the data privacy framework established under the DPD,[25] this scope does not seem to have been sufficiently achieved as for data transfer rules.

---

[21] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 233–236.

[22] Ibid., 236–258.

[23] European Commission, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final. (Brussels, 2003), 19, accessed December 28, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN. On this point see also Kuner (2017) who stated that it is "essential that there be more enforcement of international data transfer regulation. At present, EU data protection law seeks to have its cake and eat it too by containing strict legal standards, but then rarely enforcing them in practice. If data transfer regulation is to regain its legitimacy, a choice will have to be made between taking enforcement measures when the law has been violated or changing the law. Widespread enforcement of data transfer regulation might produce difficult consequences, such as the disruption of international trade and cross-border communication. But being faced with such situations may be the crucible that forces the EU to make the difficult decisions necessary to adopt a system of data transfer regulation that is both adequate in theory and effective in practice". Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," *German Law Journal* 18, no. 4 (2017): 918.

[24] European Parliament and Council of the European Union, *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 (General Data Protection Regulation)* (OJ L 119/1, 2016).

[25] As noted in 2012 by Jan Philipp Albrecht, the Rapporteur of the Committee on Civil Liberties, Justice and Home Affairs of the EU Parliament: "[s]ince the adoption of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data a lot has changed in the area of data protection, notably technological developments, increased collection and processing of personal data, including for law

Against this background, where the volume of data flow gives no sign of slowing down while the existing data transfer mechanisms seem unsuitable to deal with this flow, the importance of developing a more effective and, at the same time, more flexible, customizable and scalable framework for international data transfers seems compelling. A *safe* and at the same time *free* – or at least *smooth* – transborder data flow is, indeed, essential not only for the well-functioning of the global economy but also for giving individuals the trust and the confidence that their personal data will continue to benefit from the same level of protection regardless of data location. The results of a global survey on Internet security and trust conducted in 2019 is instructive in this respect. The survey has, indeed, shown that distrust leads people to change their online behaviour: 78% of those surveyed were concerned about their online privacy, 49% stated that their distrust in the Internet had caused them to share fewer personal information online, 39% stated that they are making a more selective use of the Internet.[26] Not by chance, one of the topics at the G20 which took place in Japan on 28 and 29 June 2019 was "Data Free Flow with Trust". In their final declaration, the G20 Leaders stressed that while "[c]ross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development", it also raises challenges pertaining to privacy, data protection and security. These challenges should be addressed so as to

enforcement purposes, with a patchwork of applicable data protection rules and globalization of markets and cooperation". European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (COM (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 2012), 209, accessed April 11, 2018, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.
Along the same lines, the European Commission stated that the "rapid pace of technological change and globalisation have profoundly transformed the scale and way personal data is collected, accessed, used and transferred. There are several good reasons for reviewing and improving the current rules, which were adopted in 1995: the increasingly globalised nature of data flows, the fact that personal information is collected, transferred and exchanged in huge quantities, across continents and around the globe in milliseconds and the arrival of cloud computing. In particular, cloud computing – where individuals access computer resources remotely, rather than owning them locally – poses new challenges for data protection supervisory authorities, as data can and does move from one jurisdiction to another, including outside the EU, in an instant. In order to ensure a continuity of data protection, the rules need to be brought in line with technological developments". Věra Jourová, *How Will the EU's Reform Adapt Data Protection Rules to New Technological Developments? - European Commission Factsheet*, 2016, accessed December 29, 2019, https://op.europa.eu/en/publication-detail/-/publication/2b2f7f00-f5b8-11e7-b8f5-01aa75ed71a1/language-en.

[26] 2019 Centre for International Governance Innovation (CIGI) – Ipsos Global Survey on Internet Security and Trust. The results of the survey are available at this link: https://www.cigionline.org/internet-survey-2019.

facilitate the free flow of data and, at the same time, "strengthen consumer and business trust". "Such *data free flow with trust* will harness the opportunities of the digital economy".[27]

In the light of the above, the overall aim of this research is to understand and highlight the main limitations of the EU data export restrictions in achieving their underlying aims and to identify what steps should be taken to protect data while allowing them to flow freely. This research hence builds on the need to ensure a free flow of data while taking into account the legitimate concerns about the risks to which data may be exposed once data are transferred across borders. The ultimate aim of this research is to identify the building blocks for a data transfer regime that may effectively achieve the objectives that stand behind the *need* for data transfer rules while addressing the limitations of the current framework. As stressed by the European Commission, "[p]rotecting and exchanging personal data are not mutually exclusive". A high level of data protection does not hinder data flow. Rather, it facilitates it "by building consumer confidence in those companies that care about the way they handle their customers' personal data".[28] As a general remark, it should be stressed from the very beginning that the analysis will be confined to the transfer of personal data for commercial purposes while international transfers for law enforcement purposes will be excluded from this analysis. These latter transfers are, indeed, not covered by the GDPR but by Directive (EU) 2016/680.[29] At the same time, this thesis will also deal with the risk that once the transfer of data for commercial purposes has started, those data may be accessed by foreign public authorities for law enforcement or national security purposes.[30]

---

[27] *G20 Osaka Leaders' Declaration*, 2019, accessed January 1, 2020, https://www.consilium.europa.eu/en/press/press-releases/2019/06/29/g20-osaka-leaders-declaration/.

[28] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 16.

[29] European Parliament and Council of the European Union, *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* (OJ L 119/89, 2016).

[30] In this respect, Advocate General Saugmandsgaard Øe has clarified that data transfer rules set out under the GDPR apply to the transfer of data even if the data that have been transferred for commercial purposes are then further processed by third country's public authorities for national security purposes. According to Advocate General Saugmandsgaard Øe, in order to determine whether the EU data transfer rules set out under the GDPR apply to the data transfer at issue, "the only factor that must be taken into consideration ... is the activity of which that transfer forms part, while the purpose of any further processing that the transferred data will undergo by the public authorities in the third

In order to address the main question that will guide this research, several other questions will need to be addressed. Chapter 2 aims to answer the following questions: *To what extent have technological developments challenged States' capability to exert their jurisdiction in the "borderless cyber world"*[31] *and what measures have been taken by States to retain their control over this dimension?* In order to answer this question, this chapter will first provide an overview of how the tensions between traditional geographic and political borders on the one hand and the un-territorial cyberspace on the other have been addressed by scholars. Moving from theory to practice, the chapter will then give some concrete examples of the increasing efforts that States have undertaken to regulate the flow of data across their borders. In particular, the first chapter aims to provide an overview of the forms, of the (possible) triggers and of the likely social and economic impacts of data localization measures, i.e., the measures that mandate that data are stored, routed or processed in servers located within national geographic borders or that limit the transfer of data to other jurisdictions. EU data transfer rules are an example of *de facto* data localization. Indeed, even though such rules do not directly impose local data storage, they may *de facto* induce companies to localize data within the EU borders as a means to avoid compliance with the strict requirements imposed by the EU data protection legislation in the event of international data transfer.

Before zooming into the intricacies of the EU data transfer rules, the following questions will be tackled: *How is the territorial scope of the GDPR defined? On what grounds is the applicability of the GDPR triggered and how far does it go in (aiming at) protecting data even when such data are processed by entities that are located outside the EU?* These questions will be addressed in chapter 3. The analysis will start from one of the basic, yet most controversial provisions of the GDPR, i.e., the territorial scope of the Regulation which was designed so as to ensure *effective* and *complete*

---

country of destination is irrelevant" (paragraph 105). In other words, according to the Advocate General, when the transfer of data forms part of a commercial activity, it is immaterial that the transferred data may be further processed by the public authorities of the third country of destination for national security purposes. Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, *Facebook Ireland and Schrems*, Case C-311/18, paragraphs 100-110.

[31] Amit M. Sachdeva, "International Jurisdiction in Cyberspace: A Comparative Perspective," *Computer and Telecommunications Law Review* 13, no. 8 (2007): 245.

protection of the right to privacy. In particular, attention will be placed on the criteria that trigger the applicability of the GDPR beyond the EU territorial borders. The boundaries of the territorial scope of the GDPR are, indeed, so loose that companies with no physical presence in the EU may be caught under the EU jurisdiction if such companies offer goods or services to data subjects in the EU or if they monitor their behaviour. Moreover, Article 3 provides that companies are subject to the GDPR if their processing activities are conducted in the context of the activities of an establishment in the European Union. In this case, the physical presence of the company in the EU seems certainly to justify the applicability of the GDPR. It might, however, seem less "justifiable" if even the presence of *one representative* of a non-EU company may trigger the applicability of the GDPR. The undesirable results of this (over)broad (extra)territorial scope will then be examined and, in particular, the enforceability problems that inevitably arise when it comes to imposing sanctions on companies located outside the EU. This analysis will prove particularly useful in order to understand to what extent the rules on the territorial scope of the GDPR and the data transfer rules overlap and interact.

Chapter 4 will then delve into the very basics of data transfer rules by addressing the following questions: *What are the main objectives underpinning the provisions on international data transfer? What is transfer under the GDPR?* This chapter is divided in two sections. The first part of the chapter aims to identify the objective(s) underpinning data transfer provisions: avoiding the circumvention of the EU data protection standards and protecting data from unauthorized and indiscriminate access by foreign public authorities. The second part will go around looking for a definition of the concept of "transfer" – and how that differs from "making data publicly available" on the one hand and "transit" on the other – so as to understand under what conditions the "movement" of data triggers the applicability of data transfer rules.

Chapter 5 will analyse the data transfer rules set out in Chapter V GDPR by tackling the following questions: *Under what mechanisms can data be transferred from the EU to third countries? How do such mechanisms differ from the data transfer provisions under the 1995 Directive? What are the main weaknesses and limitations of these mechanisms and how effective are they in achieving*

their underpinning objectives? The order of the analysis will follow the hierarchy between the transfer mechanisms set out under the GDPR (*i.* adequacy decisions under Article 45, *ii.* appropriate safeguards under Article 46 and Article 47, and *iii.* derogations under Article 49 GDPR.) and will highlight the main strengths and weaknesses of such mechanisms in enabling a smooth and "safe" data flow. The chapter will also try to make sense of the data transfer regime for processors that Article 44 has introduced by prescribing that both controllers and processors shall comply with the conditions under Chapter V. This analysis will show that a strict application of data transfer provisions by EU data processors may raise several practical problems and, under some circumstances, seems even to go against the intention of the EU legislators. Lastly, the chapter will assess to what extent, if at all, data transfer rules succeed in achieving their underpinning objectives. Indeed, on the one hand, the direct applicability of the GDPR to non-EU entities may make data transfer rules redundant in achieving the anti-circumvention objective. On the other hand, recent developments both in the EU and outside the EU seem to confirm that data location is losing its relevance as a connecting factor for grounding data disclosure requests by foreign public authorities.

After having highlighted the limitations that affect the existing data transfer regime, chapter 6 will attempt to come to a tentative conclusion about the steps that could be taken to address these limitations, and it will do so by testing the feasibility, desirability and potential effectiveness of three different possible "solutions". This chapter is divided in three parts, one for each "solution". The first part will address the following questions: *Can global convergence of data protection standards be achieved? If so, who should set these standards?* This section is built on the assumption that, if data transfer rules aim to avoid the circumvention of the law once data leave the EU borders, there would be no need for restricting data flow if the data protection principles that apply in the EU also apply to third countries. This section will explore both formal and informal (i.e., *de facto*) developments towards global convergence. In other words, it will not only provide an overview of the main initiatives that have been taken at the international level to set some common data protection standards, but it will also analyse the role of the EU data protection law as a "trendsetter": the EU

framework has, indeed, shown its power to influence not only the legislative process of third countries (which have started to adopt GDPR-like data protection legislation) but also the behaviour of commercial actors operating across various countries (which have started to adopt GDPR-compliant policies irrespective of their obligation to do so).

The chapter will then move to the second question: *To what extent can the rules on applicable law and, in particular, the broad extra-territorial scope of the GDPR replace data transfer rules?* This section aims to unpack the claim advanced by many parties that the implementation of data transfer rules would be unnecessary when data are transferred to third-country entities which are caught under the extra-territorial scope of the GDPR. This argument seems certainly sensible: if the third-country data recipient is directly subject to the GDPR, there would be no real risk that the data transferred to that recipient will be processed inconsistently with the EU data protection standards. In other words, the anti-circumvention objective which underpins data transfer rules seem to be already achieved by the broad extra-territorial scope of the GDPR. In order to test this argument, different scenarios will be analysed: (1) transfer from an EEA controller to a non-EEA processor subject to GDPR; (2) transfer from an EEA controller to a non-EEA processor *not* subject to GDPR; (3) transfer from an EEA controller to a non-EEA controller subject to GDPR; (4) transfer from an EEA controller to a non-EEA controller *not* subject to GDPR. In these scenarios, the implementation of data transfer mechanisms will prove to have an added value in protecting data compared to the "mere" extra-territorial application of the GDPR. Indeed, such mechanisms do not only *aim to* ensure the *applicability* of the EU data protection standards, but they also set out some procedural/enforcement mechanisms for ensuring the *effective implementation* of those standards.

Lastly, the potentials of the principle of accountability as an enabler of international data flow will be examined by tackling the following question: *What role can the principle of accountability play in boosting international data flow by increasing organizations' responsibility in ensuring appropriate safeguards when processing personal data?* This chapter will first give an overview of how the principle of accountability have been developed in different data protection contexts, not

only in the EU but also in some other experiences, in particular, in the Asia-Pacific Economic Cooperation (APEC) and in Canada. The purpose of this analysis is to identify the elements which should be valued and further developed as building blocks for a data transfer framework based on the principle of accountability. In this context, the principle of accountability will be mainly understood as an instrument for encouraging companies to implement the necessary measures for *ensuring* compliance with the applicable data protection rules (and for *demonstrating* such compliance) while leaving the substance of the applicable data protection rules unaltered. In other words, the principle of accountability will be understood as an instrument of data governance which mainly focus on the *measures* that shall be implemented to make compliance effective and verifiable. This section will hence aim to single out several building blocks that could be taken into account when developing an accountability-based data transfer regime starting from the experience that have been gained both within and outside the EU. The analysis will prove that a combination of *voluntary* (i.e., companies' commitment to abide by the EU data protection standards) and *regulatory* elements (i.e., some domestic legal components which should be present in third-country jurisdictions) may effectively contribute to the development of a "trusted" environment for a free flow of data. Chapter 7 will summarize the main findings of this research and the main statements that will made throughout this work.

After having identified the "what" of this research (i.e., the reasons underpinning data transfer rules, their flaws and the steps that should be taken to develop a pro-growth and pro-future data transfer regime), and the "why" (i.e., the need to ensure an agile flow of data without undermining the protection of those data), the third point of the "Eternal Triangle of Intellectual Inquiry" needs to be defined: the "how" of this research.[32] This research combines doctrinal legal research[33] with non-doctrinal legal research which, following the categorisation of Dobinson and Johns (2017), can be

[32] Paul Roberts, "Interdisciplinarity in Legal Research," in *Research Methods for Law*, ed. Michael McConville and Chui, Second edition. (Edinburgh: Edinburgh University Press, 2017), 100–101.

[33] Ian Dobinson and Francis Johns, "Legal Research as Qualitative Research," in *Research Methods for Law*, ed. Michael McConville and Wing Hong Chui, Second edition. (Edinburgh: Edinburgh University Press, 2017), 21.

grouped in problem, policy and law-reform legal research.[34] Indeed, this research not only asks and describes what the data transfer rules look like in the EU data protection framework but also aims at understanding the flaws that affect such rules, the policies and the objectives underpinning such rules and it will reach a tentative conclusion about how these rules could be reformed. Both descriptive (or expository) and evaluative components will hence be intertwined throughout the whole study.[35]

The analysis will be conducted on the basis of both normative and non-normative sources. As for normative sources, primary attention will perforce be placed on the provisions set out under the GDPR, under the 1995 Directive (not only in their current form but also how the wording of their provisions has changed over the legislative procedure) and under the relevant legal acts that have been adopted pursuant to these pieces of law.[36] The analysis of the text of the law will often need to be backed up by the analysis of the main judgments of the Court of Justice of the European Union in which the provisions examined have been interpreted and applied. It should however be noted that the references to the case-law included in this work concern the 1995 Directive and not the GDPR. This "transfer" of the existing case-law *on* the 1995 Directive *to* the GDPR derives from the fact that, at the time of writing, no judgement has been delivered by the Court of Justice of the European Union which directly concern the interpretation and application of the data transfer rules as currently shaped under the GDPR. The reason why the existing case-law on the 1995 Directive retains its relevance under the GDPR is twofold: firstly, the case-law that will be analysed in this work concerns some legal acts that have been adopted under the 1995 Directive but which remain valid under the GDPR;[37] secondly, the case-law that will be examined concerns the interpretation of some provisions of the 1995 Directive which have remained unchanged under the GDPR, in particular with reference to the concept of "transfer" (chapter 4) and some of the wording that is used to define the territorial scope

[34] Ibid., 22.

[35] Ibid., 35–36. See also, Robert Cryer et al., *Research Methodologies in EU and International Law*, 1st ed. (Oxford: Hart Publishing, 2011), 9.

[36] Among others, the decisions of the European Commission has adopted pursuant to Article 25(6) and pursuant to Article 26(4) of the 1995 Directive (see paragraphs 5.4.3. and 5.5.1.2.).

[37] Again, the decisions of the European Commission adopted pursuant to Article 25(6) and pursuant to Article 26(4) of the 1995 Directive.

of the EU data protection legislation (chapter 3). Moreover, even if most of the attention is placed on the EU data protection framework, this research also includes hints on the data protection legislation that has been developed in some non-EU countries, as well as an overview of the initiatives that have been taken at the international level in the data protection field, in particular, by the United Nations (UN), the Council of Europe and the Organisation for Economic Cooperation and Development (OECD).

Several non-normative sources have also been consulted, including textbooks, journal articles and other scholarly writings, position papers and communications from the EU institutions, public statements by States' or EU representatives, working documents, press releases, policy briefs, presentations at conferences, blogs, the "news" section and client alerts of the major law firms dealing with data protection and cybersecurity. Most importantly, an essential role in guiding the interpretation of the DPD and the GDPR provisions is played by the opinions and the guidelines of the Article 29 Working Party (A29WP). The A29WP is an independent European body which was established under Article 29 of the 1995 Directive and which is in charge of ensuring the consistent application of the EU data protection rules across the EU. The A29WP ceased to exist upon the entry into force of the GDPR which has replaced the A29WP with the European Data Protection Board (EDPB). Equally, important guidance is also offered by the guidelines, the reports and the opinions of the European Data Protection Supervisor (EDPS), which is the European Union independent data protection authority.

Moreover, the privacy policies as well as the data processing agreements (DP Agreements) pursuant to Article 28 GDPR that have been adopted by some of the major commercial actors, in particular cloud service providers (Google, Amazon Web Services, Rakspace, Oracle, OVH, Salesforce, Box), have been analysed so as to understand how these actors have "adapted" to the EU data protection legislation. Lastly, even if this research mostly deals with "words", some numbers and statistics will also be mentioned to support some of the arguments that will be made or to explain

some of the phenomena that will be explored,[38] in particular the data localization phenomenon analysed in chapter 2. The data collected fall under the category of "secondary" data since they have not been generated during this research (in which case, they would be "primary" data), but they have been obtained by other researchers or official statistics.[39]

Before moving to the next chapter, it is important to define the key data protection terms that will be used throughout this work. Since this research aims to delve into the EU data protection framework, the definitions provided under Article 4 GDPR will be followed. In particular, "personal data" is defined as "any information relating to an identified or identifiable natural person". The natural person to which data refer is called "data subject".[40] "Processing" of personal data is defined in a very broad fashion. This activity is, indeed, described 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[41] Such processing activities may be conducted by a natural or legal person, public authority, agency or other body acting as a data controller or as a data processor. The difference between a data controller and a data processor is that while the data controller determines, "alone or jointly with others, ... the purposes and means of the processing of personal data",[42] the data processor "processes personal data on behalf of the controller".[43] Some other working definitions will be provided throughout this thesis.

[38] Wing Hong Chui, "Quantitative Legal Research," in *Research Methods for Law*, ed. Michael McConville and Chui, Second edition. (Edinburgh: Edinburgh University Press, 2017), 50.
[39] Ibid., 59–60.
[40] Article 4(1) GDPR.
[41] Article 4(2) GDPR.
[42] Article 4(7) GDPR.
[43] Article 4(8) GDPR.

2. The Hows, the Whys and the Wherefores of Data Localization

2.1. Introduction

The aim of this chapter is to understand to what extent technological developments have challenged States' capability to exert their jurisdiction in the "borderless cyber world"[44] and what measures have been taken by States to retain their control over this dimension. The analysis that will be conducted in this chapter aims to show that the EU data transfer rules mirror States' attempts to exert their jurisdiction over the *un*-territorial cyberspace (and over the data that move across it). This chapter will first provide an overview of the different theories that have been developed by scholars about the relationship between territorial sovereignty and cyberspace. This analysis will show that calls for the independence of cyberspace from governments' assertions have been superseded by a wide literature that has recognized the applicability of territorial sovereignty to cyberspace by virtue of the inextricable links between cyberspace and its underlying physical infrastructure. Concrete examples of States' attempts to exert their jurisdiction over cyberspace and, precisely, over data that move across it, will then be explored. Indeed, States have increasingly resorted to measures that aim to retain control over what has been defined as "the new oil of the digital economy".[45] These measures have been labelled as "data localization laws". Data localization laws take different forms, and these different forms (may) hide different underlying goals that scholars have attempted to unveil. EU data transfer rules are an example of *de facto* data localization. Indeed, although such rules do *not* include an explicit and outright ban on transborder data flow, by making international transfer conditional upon compliance with some strict requirements, they may induce companies to localize data within the EU as an easy "way out" from such requirements.

[44] Sachdeva, "International Jurisdiction in Cyberspace: A Comparative Perspective," 245.

[45] Joris Toonders, "Data Is the New Oil of the Digital Economy," *WIRED*, accessed December 31, 2017, https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/. The expression "data is the new oil", however, dates back at least to 2006. See, for example, Michael Palmer, "Data Is the New Oil," *ANA Marketing Maestros*, last modified November 3, 2006, accessed February 16, 2018, http://ana.blogs.com/maestros/2006/11/data_is_the_new.html.

2.2. Territorial Sovereignty Versus *Un*-territorial Cyberspace

The respect for territorial sovereignty between independent States "is an essential foundation of international relations"[46] and its preservation is a vital goal for international organizations as well States individually.[47] As affirmed by Judge Max Huber in the *Palmas Island* arbitration award, "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State".[48] Sovereignty, as inherent to statehood, implies that States enjoy the exclusive right and the (nearly)[49] absolute authority to exercise *jurisdiction* on objects and persons within their geographic borders, including the right to control the access to, the transit through and the exit from their territory.[50] The notion of territorial sovereignty is therefore strictly intertwined with the notion of jurisdiction.[51] The term jurisdiction traditionally indicates the authority to prescribe, enforce and adjudicate. Precisely, the jurisdiction to prescribe entails the right and the power of a State to prescribe normative standards, enforcement jurisdiction indicates the power to enforce the law by means of investigations, prosecution and coercive measures, while adjudicative jurisdiction refers to the power to adjudicate upon a matter.[52]

---

[46] *Corfu Channel* (U.K. v. Alb.), 1949 I.C.J. 6, 35 (Apr. 9).

[47] Patrick W. Franzese, "Sovereignty in Cyberspace: Can It Exist?," *Air Force Law Review* 64, no. 1 (2009): 7, accessed January 30, 2018, https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist.

[48] *Island of Palmas* (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

[49] Eric Talbot Jensen, "Cyber Sovereignty: The Way Ahead," *Texas International Law Journal* 50, no. 2 (2015): 283, accessed February 11, 2019, https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1239&context=faculty_scholarship. Sovereignty can be subject to the exceptions prescribed by conventional as well as customary rules of international law (e.g., actions of the UN Security Council, the law of armed conflict and the respect for fundamental rights).

[50] Among others, Rule 1.4, Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), accessed January 30, 2018, https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf; Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," *International Law Studies* 123, no. 89 (2013): 124, accessed January 30, 2018, http://stockton.usnwc.edu/cgi/viewcontent.cgi?article=1027&context=ils.

[51] M. Zoetekouw, "Ignorantia Terrae Non Excusat" (Presented at the Crossing Borders: Jurisdiction in Cyberspace Conference, Amsterdam, the Netherlands, March 2016), 3, accessed November 2, 2019, https://c.ymcdn.com/sites/www.iisfa.net/resource/resmgr/Slide_seminari/Convegno_Milano/c-mzoetekouw-ignorantia-terr.pdf; Anna-Maria Osula, "Transborder Access and Territorial Sovereignty," *Computer Law & Security Review* 31 (2015): 721.

[52] Dan Jerker B. Svantesson and Felicity Q.C. Gerry, "Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond," *Computer Law & Security Review* 31 (2015): 480.

Technological developments have challenged States' capability to exert their jurisdiction in the "borderless cyber world"[53] thus opening the door to calls for the independence of cyberspace from national frontiers, and hence from governments' regulation. As emphatically expressed by Barlow (1996) in his Declaration of Independence of Cyberspace, the "legal concepts of property, expression, identity, movement, and context do not apply" to cyberspace. These concepts "are all based on matter, and there is no matter" in cyberspace.[54] On these premises, several authors have theorized the "cyberspace self-governance movement". Among these scholars, Johnson and Post (1996) argued that cyberspace undermines the feasibility of a rule-making system based on geographic boundaries.[55] Indeed, by challenging the traditional and general correspondence between physical and legal borders, the rise of global computer-based communications has broken the bond between geographic location and the capacity, as well the legitimacy, of national governments to exercise control over online behaviours.[56] Cyberspace cannot be governed by territorially-based rules. Rather, it should be left to develop its own rule sets and institutions[57] and national authorities should yield to the emergence of this new self-regulatory structure.[58]

A second theory that several scholars have put forward in this lingering debate about the applicability of territorial sovereignty to cyberspace is that this new dimension should be assimilated to the high sea, the Antarctic and the outer space. By virtue of this assimilation, some scholars consider cyberspace as a global common (or *res communes omnium*), meaning that it belongs to everybody but can be seized by nobody. The idea of cyberspace as a global common was advanced by several authors. Among others, Menthe (1998) argued that cyberspace is a fourth international

[53] Sachdeva, "International Jurisdiction in Cyberspace: A Comparative Perspective," 245.

[54] John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation*, last modified January 20, 2016, accessed January 31, 2018, https://www.eff.org/it/cyberspace-independence.

[55] David R. Johnson and David Post, "Law And Borders – the Rise of Law in Cyberspace," *Stanford Law Review* 48, no. 5 (1996): 1367, accessed January 31, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535.

[56] Ibid., 1370.

[57] "Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world". Ibid., 1401.

[58] Ibid., 1367.

space together with high seas, outer space and Antarctica.[59] This assimilation may sound surprising considering the blatant differences between these four dimensions: the high sea, the Antarctic and the outer space are three different physicalities while cyberspace is a nonphysical space. At the same time, however, Menthe stressed that what makes these dimensions part of the same category is not their physical nature but their "sovereignless quality".[60] Cyberspace should therefore be governed by rules that resemble those applying to the other international spaces. In particular, nationality and not territory should be the criteria for asserting jurisdiction in cyberspace. As the nationality of the registry of the aircrafts governs in outer space, the nationality of the vessels at sea, and the nationality of the base in Antarctica, the nationality principle should be the primary rule for asserting jurisdiction in cyberspace.[61] Until an international treaty specifies what carries nationality in cyberspace, the nationality principle should be driven by the nationality of the persons who carry out actions in cyberspace: "we may not know 'where' a webpage is, but we know *who* is responsible for it".[62]

However, calls for the immunity of cyberspace from governments' interferences have recently been superseded by a wide literature that militates in favour of the applicability of territorial sovereignty to cyberspace. The main argument advanced in support of this theory is that cyberspace could not exist without the underlying physical infrastructure. Cyber infrastructure[63] is composed of physical components, such as servers, computers and cables that are located within territorial borders and linked to the national electric grid:[64] "the fact that cyber infrastructure located in a given State's territory is linked to the global telecommunications network cannot be interpreted as a waiver of its sovereign rights over that infrastructure".[65] This increasingly accepted idea has been confirmed by

[59] Darrel C. Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces," *Michigan Telecommunications and Technology Law Review* 4, no. 1 (1998): 70, accessed January 31, 2018, https://repository.law.umich.edu/cgi/viewcontent.cgi?referer=https://www.google.co.uk/&httpsredir=1&article=1163&context=mttlr.

[60] Ibid., 85.

[61] Ibid., 83.

[62] Ibid., 93 (italics mine).

[63] The glossary of technical terms of the *Tallinn Manual* defines cyber infrastructures as "the communications, storage, and computing resources upon which information systems operate".

[64] von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," 126; Jensen, "Cyber Sovereignty: The Way Ahead," 296.

[65] Rule 1(10), Schmitt (ed), *Tallinn Manual*.

the *Tallinn Manual* (2013) that, although not binding,[66] provides that a "State may exercise control over cyber infrastructure and activities within its sovereign territory".[67] In response to the difficulties of confining the world wide web bubble within national borders which are at the basis of the "cyberspace as *res communes omnium*" theory, the authors of the *Tallinn Manual* emphasized that, even though States cannot assert their sovereignty over cyberspace as a whole, they can still exert their control over the infrastructures placed on their territory, as well as over the activities carried out by means of those cyber infrastructures.[68]

Likewise, von Heinegg (2013) affirmed that, even though the characterization of cyberspace as a global common is "logical" and hence correct, this classification only means that cyberspace in its entirety cannot be object of appropriation by one single State or a group of States while components of cyberspace are not immune from national sovereignty.[69] States are hence entitled to exercise their exclusive jurisdiction over cyber infrastructures located in their land area, internal and archipelagic waters, territorial sea and national airspace, as well as over activities linked to those infrastructures.[70] No matter who is the owner of these infrastructures (whether the State or private companies or individuals) and where they are located (whether within their territorial borders, on board of vessels flying their flag or aircrafts and other platforms registered in that State).[71] Rule 1(5) of the *Tallinn Manual*, indeed, stresses that territorial sovereignty protects cyber infrastructures no matter whether they belong "to the government or to private entities or individuals",[72] while Rule 3(3) prescribes that cyber infrastructures located in high seas, international airspace, or in outer space are subject to "the flag State principle in the case of ships and on the State of registration for aircrafts and space objects".[73]

---

[66] The *Tallinn Manual* was prepared by a group of experts invited by the NATO's Cooperative Cyber Defence Centre of Excellence. It is an academic and therefore non-binding study on the international law that governs cyber warfare.

[67] Rule 1, Schmitt (ed), *Tallinn Manual*.

[68] Rule 1(1), Ibid.

[69] von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," 125–126.

[70] Ibid., 128. See also Rule 1(3), Schmitt (ed), *Tallinn Manual*.

[71] von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," 129.

[72] Rule 1(5), Schmitt (ed), *Tallinn Manual*.

[73] Rule 3(3), Ibid.

2.3. Data Localization and its Triggers

If territory allows States to easily assert (and effectively exert) their jurisdiction, and if "black gold" as "the world's most valuable resource" has been "surpassed by data",[74] States' increasing efforts to control and regulate data entering and leaving their territory should come as no surprise. Indeed, it is not historically unprecedented that States try to retain control over the resources on which they depend.[75] Over the past few years, States have increasingly resorted to the adoption of the so-called "data localization laws". Data localization laws are also referred to as "data sovereignty laws".[76] Indeed, by mandating that data are stored, routed or processed in servers located within national geographic borders or by limiting the transfer of data to other jurisdictions, they reflect national authorities' intent to assert their sovereignty – and therefore their control and regulations – over data. Precisely, data localization laws can be defined as those "laws that limit the storage, movement, and/or processing of data to specific geographies and jurisdictions, or that limit the companies that can manage data based upon the company's nation of incorporation or principal sites of operations and management".[77]

Data localization encompasses different types of policies. Firstly, there are measures that require that data are stored and/or processed in servers located within the territory of a nation ("localized data hosting").[78] Secondly, there are requirements that fall under the label "localized data

[74] Ramona Pringle, "'Data Is the New Oil': Your Personal Information Is Now the World's Most Valuable Commodity," *CBC News*, last modified August 25, 2017, accessed December 31, 2017, http://www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677.

[75] Eric J. Novotny, "Transborder Data Flows and International Law: A Framework for Policy-Oriented Inquiry," *Stanford Journal of International Law* 16, no. 2 (1980): 161. With reference to less developed countries, Bortnick (1981) stated that "[i]nformation is a resource that yields economic, political, and technological advantages. National sovereignty, in the context of information, refers to a country's desire to control its own information resources and the advantages flowing therefrom. Other countries' use of these resources threatens less developed countries' national sovereignty by undermining this control. The threat is of particular concern to developing nations because they lack the data processing and telecommunication tools to fully exploit their information resources". Jane Bortnick, "International Information Flow: The Developing World Perspective," *Cornell International Law Journal* 14, no. 2 (1981): 338.

[76] Courtney M. Bowman, "A Primer on Russia's New Data Localization Law," *Privacy Law Blog*, last modified August 27, 2015, accessed December 31, 2017, https://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/.

[77] Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," *Lawfare Research Paper Series* 2, no. 3 (2014): 3, accessed December 30, 2017, https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf.

[78] John Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?," *International Journal of Law and Information Technology* 25, no. 3 (2017): 214.

routing",[79] and that mandate changes in the network architecture so as to confine the Internet traffic within a certain region. Thirdly, there are requirements that data are processed by companies located in a specific jurisdiction. Fourthly, there are policies that select companies that can handle data on the basis of their nation of incorporation. Fifth, there are restrictions on cross-border data flow.[80]

Several scholars attempted to unveil the sentiments and the goals that (may) have motivated the adoption of data localization measures. In many cases, data localization measures respond to privacy and information security concerns. Data localization laws are often a response to the fear that data could be imperilled if they are stored and processed outside States' geographic and political borders. This fear started to be perceived from the 1970s when the differences between the approaches to privacy adopted in different States started to emerge. In the light of these differences, many governments feared that the transfer of personal data to third countries where data protection laws are weaker or completely absent could lead to the "erosion of privacy protection available to individuals in their home countries".[81] Restrictions to cross-border data flow hence emerged as an expedient for protecting data from being moved from States with higher data protection to regions that could have become "data havens" due to their lax regulation.[82] In 1970, for example, Kerstin Amer, a representative of the Swedish Government, justified the implementation of restrictions to cross-border data flow by saying: "we do not really trust the Data Acts in other countries or ... we understand that there are none at all. So we feel unprotected in those countries with our data – walking down Fifth Avenue in our underwear".[83] As it will be discussed in chapter 4, the restrictions to cross-border

---

[79] Ibid.

[80] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, *Internet Fragmentation: An Overview* (Future of the Internet Initiative White Paper, World Economic Forum, 2016), 41, accessed February 20, 2018, http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[81] Rein Turn, "An Overview of Transborder Data Flow Issues" (Presented at the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1980), 3–4, accessed February 7, 2018, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6233696.

[82] Christopher Millard, *Legal Protection of Computer Programs and Data* (London: Sweet & Maxwell, 1985), 211. See also Frits W. Hondius, "Data Law in Europe," *Stanford Journal of International Law* 16, no. 2 (1980): 102–103.

[83] Quoted in Christopher Kuner et al., "Internet Balkanization Gathers Pace: Is Privacy the Real Driver?," *International Data Privacy Law* 5, no. 1 (February 1, 2015): 1, accessed January 30, 2018, http://dx.doi.org/10.1093/idpl/ipu032. For other examples of early restrictions to transborder data flow in Europe see Eric J. Novotny, "Transborder Data Flows and International Law: A Framework for Policy-Oriented Inquiry," *Stanford Journal of International Law* 16, no. 2 (1980): 164 and Mark B. Feldman and David R. Johnson, "National Regulation

data transfer that have been implemented by the European Union in 1995 reflect the same concern. Data transfer rules were, indeed, adopted as a means to avoid the circumvention of the law once data are transferred to another jurisdiction.[84]

Moreover, besides preventing data from being transferred to untrustworthy jurisdictions with weaker data protection standards,[85] after Snowden's revelations, data localization requirements started to be seen as a means to protect citizens' data from falling in the hands of foreign intelligence agencies. The idea is that, by limiting the transit of data through foreign territories, data localization would contribute to making foreign illegitimate wiretapping more costly and technically burdensome.[86] For instance, in 2014, Chancellor Angela Merkel, together with the French President Francois Hollande, proposed to build a "Schengen area routing", i.e., a regional network confined within the EU countries that have already agreed to abolish border controls (notably, with the exclusion of the UK that, as the Snowden's revelations have shown, has closely cooperated with the U.S. mass harvesting of data)[87] "so that one shouldn't have to send emails and other information across the Atlantic".[88] By the same token, BRICS States (Brazil, Russia, India, China and South Africa) planned to build a brand new Internet network "'free of US eavesdropping' which via legislative mandates will also force the likes of Google, Facebook and Yahoo to store all data generated by BRICS nations locally, shielding it from" US National Security Agency's (NSA)

---

of Transborder Data Flows," *North Carolina Journal of International Law and Commercial Regulation* 7, no. 1 (1982): 15–21.

[84] See, among others, Christopher Kuner, "Data Nationalism and Its Discontents," *Emory Law Journal* 64 (2015): 2093, accessed January 8, 2018, http://law.emory.edu/elj/_documents/volumes/64/online/kuner.pdf.

[85] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 29; Joshua Meltzer, *The Internet, Cross-Border Data Flows and International Trade* (Issues in Technology Innovation, Center for Technology Innovation at Brookings, 2013), 6–7, accessed November 2, 2019, https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf.

[86] Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?," 228. See also, Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64 (2015): 714–718, accessed January 7, 2018, http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

[87] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 11–12. See also, W. Kuan Hon et al., *Policy, Legal and Regulatory Implications of a Europe-Only Cloud* (Legal Studies Research Paper 191/2015, Queen Mary University of London, School of Law, 2015), 2–5, accessed May 4, 2018, http://www.picse.eu/sites/default/files/PolicyLegalandRegulatoryImplicationsof%20EuropeOnlyCloud.pdf.

[88] "Merkel and Hollande Mull Secure European Communication Web," *Deutsche Welle*, last modified February 16, 2014, accessed December 31, 2017, http://www.dw.com/en/merkel-and-hollande-mull-secure-european-communication-web/a-17435895.

snooping.[89] Along the same lines, in Brazil, Snowden's revelations triggered proposals aimed at storing data about Brazilian citizens on servers located on the Brazilian soil.[90]

Somewhat more cynically, some even argued that, instead of protecting data from foreign intelligence access, data localization is mainly motivated by governments' intention to make access to their citizens' data logistically easier for *domestic* intelligence agencies. Indeed, despite the several public protestations against NSA massive intelligence collection programs, other States also maintain robust intelligence apparatus and it is reasonable to think that governments will push for enhancing their surveillance capacities.[91] For example, when in 2013, the biggest German telecommunications company Deutsche Telekom proposed a national routing scheme aimed at restricting Internet traffic within the country's borders,[92] many feared that this proposal, rather than better protecting privacy, could lead to the enhancement and the centralization of the surveillance capabilities of German intelligence agencies.[93] Amelia Andersdotter, the representative of the Pirate Party in the European Parliament, clearly expressed her scepticism about the exact scope of the proposed German Internet when she asked: "[w]hy should we believe that the limitation of Internet traffic to Germany and Europe means the problem is solved? To me it seems very vague, if not suspect".[94] Such concerns are justified considering that data localization offers opportunities for the enhancement of surveillance capacities of domestic intelligence agencies by requiring that data are stored in local

[89] Paul Joseph Watson, "BRICS Countries Build New Internet to Avoid NSA Spying," *Infowars*, October 24, 2013, accessed January 25, 2018, https://www.infowars.com/brics-countries-build-new-internet-to-avoid-nsa-spying/. The project was however stalled in 2015, Stacia Lee, "International Reactions to U.S. Cybersecurity Policy: The BRICS Undersea Cable," *The Henry M. Jackson School of International Studies*, January 8, 2016, accessed October 27, 2019, https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/.

[90] This proposal was eventually dropped. Indeed, many argued that this proposal would have increased costs on users without guaranteeing effective protection against foreign actors. Hon et al., *Policy, Legal and Regulatory Implications of a Europe-Only Cloud*, 14. See also, "Brazil Plans to Go Offline from US-Centric Internet," *The Hindu*, September 17, 2013, accessed January 26, 2018, http://www.thehindu.com/news/international/world/brazil-plans-to-go-offline-from-uscentric-internet/article5137689.ece; T. A. Ridout, "Marco Civil: Brazil's Push to Govern the Internet," *Huffington Post*, October 22, 2013, accessed January 26, 2018, https://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html.

[91] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 24–25.

[92] Richard Adhikari, "Deutsche Telekom Pitches NSA-Free German Internet," *TechNewsWorld*, last modified October 26, 2013, accessed January 3, 2018, https://www.technewsworld.com/story/79286.html.

[93] Alex Evans, "Can Germany Really Keep Bytes within Its Borders?," *The Local*, November 29, 2013, accessed January 3, 2018, https://www.thelocal.de/20131129/german-email-providers-unite-german-internet-against-nsa.

[94] Gabriel Borrud, "Germany Looks to Erect IT Barrier," *Deutsche Welle*, last modified November 4, 2013, accessed January 3, 2018, http://www.dw.com/en/germany-looks-to-erect-it-barrier/a-17203480.

servers to which domestic intelligence agencies have *easier* access, or that data are held by domestic firms over which they have *greater* coercive powers. Moreover, by enhancing their control over data held domestically, data localization is deemed to raise intelligence agencies' bargaining power in their information sharing programs with foreign intelligence services and with the NSA in the first place.[95]

In addition to this, data localization is deemed to facilitate law enforcement agencies' activities by giving them easier access to evidence – especially digital evidence – that is necessary for conducting their criminal investigations. Indeed, law enforcement authorities struggle to gain access to data stored in foreign jurisdictions. Traditional tools for gaining (lawful) access to evidence held abroad have proved extremely slow and inefficient in the digital sphere and, hence, incompatible with the necessity to allow a timely investigation and a swift prosecution of crimes.[96] The cyber dimension poses, in fact, several challenges to the traditional approach to international law-enforcement cooperation. As some experts have argued, "[t]he traditional mechanisms of international cooperation, including letters rogatory, mutual assistance and other formalities with roots in the 19th century and earlier, are ill-suited to an era in which offences can be, and are, committed from across the world in real time".[97]

In particular, mutual legal assistance treaties (MLATs) are often invoked in order to gain access to data held in a foreign jurisdiction. MLATs are agreements under which one State (the requested State) can be compelled by another States (the requesting State) to perform some investigative activities.[98] However, MLATs "have been notoriously complex, slow, and

[95] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 25. A similar argument was advanced by John Selby who argued that many data localization policies have been driven not only by States' attempt to reduce their comparative disadvantage in the data hosting industry, but also by the attempt "to reduce their comparative disadvantage in Internet signals intelligence" *vis-à-vis* the US. Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?," 213.

[96] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 26.

[97] Kim-Kwang Raymond Choo, Russell G. Smith, and Rob McCusker, *Future Directions in Technology-Enabled Crime: 2007–09* (Research and Public Policy Series No. 78, Australian Institue of Criminology, 2007), 72, accessed January 23, 2018, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.4136&rep=rep1&type=pdf.

[98] Bert-Jaap Koops and Morag Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law* (Tilburg Law School Legal Studies Research Paper Series No. 05/2016,

bureaucratic"[99] and hence unable to provide the requesting authorities with prompt access to the sought-after evidence. A request under the MLA system usually takes months to be fulfilled, which is clearly at odds with the necessity to secure and preserve critical evidence,[100] especially when it comes to volatile digital evidence.[101] This unease with the inefficiencies of the MLA regime was also expressed by the US Government in the *Microsoft* case, which initiated in 2013 when Microsoft refused to disclose to the US authorities the content related to an email account because the requested data were stored in a servers located in Dublin: "an MLAT request typically takes months to process, with the turnaround time varying widely based on the foreign country's willingness to cooperate, the law enforcement resources it has to spare for outside requests for assistance, and the procedural idiosyncrasies of the country's legal system"[102] (on the Microsoft's Search Warrant Case se also 5.8.2.).

Moreover, since data are constantly shifted from one place to another and often replicated or distributed in several places simultaneously, identifying the competent authorities to which a mutual legal assistance request should be sent represents a major challenge for law enforcement authorities.

2014), 24, accessed January 23, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263. As clearly explained by Gail Kent, "Mutual Legal Assistance is an agreement, usually by treaty, between two or more countries to provide assistance to each other on criminal legal matters. The types of assistance that can be provided through MLA include: service of documents; search and seizure; restraint and confiscation of proceeds of crime; provision of telephone intercept material; and the facilitation of taking of evidence from witnesses". Gail Kent, "Sharing Investigation Specific Data with Law Enforcement - An International Approach," *Stanford Public Law Working Paper* (February 14, 2014): 5, accessed January 23, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413.

[99] Ian Walden, "Law Enforcement Access to Data in Clouds," in *Cloud Computing Law*, ed. Christopher Millard (Oxford: Oxford University Press, 2013), 297.

[100] Andrew K. Woods, *Data Beyond Borders. Mutual Legal Assistance in the Internet Age* (Global Network Initiative, 2015), 3, accessed January 23, 2018, http://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1517&context=law_facpub.

[101] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, 2013, 197, accessed January 23, 2018, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. "The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular". Council of Europe, Cybercrime Convention Committee, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime* (Strasbourg, 2014), 123, accessed February 21, 2018, https://rm.coe.int/16802e726c. See also, John Miller and Sana Ali, "No Safety in Silos," *Information Technology Industry Council*, last modified August 16, 2016, accessed February 19, 2018, http://www.itic.org/news-events/techwonk-blog/no-safety-in-silos?.

[102] United States Government, *Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within Its Custody and Control, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* (1:13-mj-02814, 2014), 25–26, accessed January 23, 2018, https://blogs.microsoft.com/wp-content/uploads/sites/149/2017/02/the-government-brief.pdf.

Indeed, in a system where location of the sought-after evidence is the guiding principle for determining the jurisdiction that applies to that evidence, the "loss of location"[103] of data, or better, the "loss of knowledge of location"[104] of data hampers law enforcement authorities' capacity to identify the sovereign State to which they would have to address their request for mutual assistance.[105] As a further element of complexity, MLATs, as any other treaties, are not universal,[106] and companies may be tempted to take advantage of these gaps. Once again, this concern was expressed by the US government in the Microsoft's Search Warrant Case: "there are many countries in the world that do not even have MLATs with the Unites States. A U.S. provider could easily choose to locate its user data in such a country, either for business reasons or for the specific purpose of evading the reach of U.S. law enforcement".[107] Against this background, by mandating domestic data storage, data localization would free law enforcement authorities from their burdensome dependence on outdated mechanisms for gathering evidence stored offshore.[108] Localized routing was, for example, proposed by Nugraha et al. (2015) as a requirement for building Indonesian data sovereignty since it "would help ensure an Indonesian law enforcement agency can better perform investigation because the data flows are localised within the country, which is subject to national laws. Localised routing helps to control data generated in or passing through the national communications infrastructure".[109]

---

[103] Council of Europe, *Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?*, 2010, 5–6, accessed February 11, 2019, https://rm.coe.int/16802fa3df.

[104] Koops and Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law*, 9.

[105] Council of Europe, *Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?*, 5–6. See also, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, 216–218.

[106] Alan McQuinn and Daniel Castro, *How Law Enforcement Should Access Data Across Borders* (Information Technology and Innovation Foundation, 2017), 7, accessed January 23, 2018, http://www2.itif.org/2017-law-enforcement-data-borders.pdf.

[107] United States Government, *Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within Its Custody and Control, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 26.

[108] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 26. See also, Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?," 230.

[109] Yudhistira Nugraha, Kautsarina, and Ashwin Sastrosubroto, "Towards Data Sovereignty in Cyberspace" (Presented at the Third International Conference of Information and Communication Technology, Bali, Indonesia, May 2015), 5, accessed February 15, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2610314.

Moreover, information security is increasingly intertwined with national security. Indeed, although the Internet offers more opportunities for enhancing security and welfare, it also makes data more exposed to potentially destructive cyberattacks by foreign governments, individuals and non-governmental criminal networks. As stated by the U.S. Defence Secretary Panetta in 2012, "[t]he Internet is open. It's highly accessible, as it should be. But that also presents a new terrain for warfare. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens".[110] The same concern was expressed in February 2017 by Brad Smith, the president of Microsoft Corporation, when he stressed the need to adopt a Digital Geneva Convention so as to address the increasing governments' attempts to exploit the cyberspace to pursue their own national security objectives.[111] In this framework, the need to protect national critical networks, and national security in cyberspace more broadly, may impact on States' willingness to regulate and restrict data flow across their borders.[112]

At the same time, as several scholars have highlighted, privacy and information security are often only a smokescreen for furthering other covert purposes. According to many, one of these purposes is protectionism, or better "data protectionism",[113] also known as "data mercantilism".[114] The idea is that data localization favours domestic information technology sector by placing heavy burdens of regulatory compliance on foreign companies.[115] Protectionist sentiments mainly derive

---

[110] Leon E. Panetta, "Remarks on Cybersecurity to the Business Executives for National Security" (New York City, October 11, 2012), accessed January 25, 2018, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[111] Brad Smith, "The Need for a Digital Geneva Convention" (Presented at the RSA Conference, San Francisco, California, February 14, 2017), accessed February 9, 2018, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[112] Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 7.

[113] Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, 2015, 3, accessed January 22, 2018, https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf. The same expression was used by Michael D. Kirby back in 1980 when he defined "data protectionism" as "[l]egislation, nominally for the purpose of data protection, [that] could actually have such objectives as the protection of domestic employment, local technology and expertise, home industries, national culture, language, and sovereignty". Michael D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy," *Stanford Journal of International Law* 16, no. 2 (1980): 28.

[114] Stephen J. Ezell et al., *Localization Barriers to Trade: Threat to the Global Innovation Economy* (The Information Technology & Innovation Foundation, 2013), 18, accessed January 22, 2018, http://www2.itif.org/2013-localization-barriers-to-trade.pdf.

[115] "Meeting the Challenge of Data Localization Laws," *Servers.Global*, November 30, 2016, accessed December 31, 2017, https://www.servers.global/meeting-the-challenge-of-data-localization-laws/.

from companies' as well as governments' desire to gain a competitive advantage in the IT market that has been long dominated by US technology giants.[116] Nothing surprising considering that Google has the 75.48% of the search engine market share,[117] that Facebook is the most popular social network with over 2.41 billions of monthly active users as of June 2019,[118] that Amazon is one of the largest retailers worldwide,[119] and that all these companies, together with Apple and Microsoft, dominate the tech industry.[120] Since tariffs and other traditional protectionist tools are not as effective when it comes to digital economic activities,[121] data localization seems to be a relatively easy option for overcoming the inability of several nations to develop their own domestic IT market to confront the "American Internet hegemony".[122] Besides increasing domestic companies' share of the national IT market by reducing the prominence of foreign tech firms, data localization supposedly creates incentives for companies to build new data centres thus favouring local investments and, in turn, the creation of high-paying jobs opportunities for the local population.[123] Indeed, as noted by Millard back in 1985, the fact that most of the computer services production is located in a few countries – and in particular in the United States – also implies that most of the related jobs are located in those few countries. Restrictions on transborder data flow have hence started to emerge as non-tariff trade

[116] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 23.

[117] "Search Engine Market Share," accessed October 27, 2019, https://goo.gl/vb1Gof.

[118] "Facebook Newsroom," 2019, accessed October 27, 2019, https://newsroom.fb.com/company-info/. Rosamond Hutt, "The World's Most Popular Social Networks, Mapped," *World Economic Forum*, last modified March 20, 2017, accessed January 15, 2018, https://www.weforum.org/agenda/2017/03/most-popular-social-networks-mapped/.

[119] Lauren Gensler, "The World's Largest Retailers 2017: Amazon & Alibaba Are Closing In On Wal-Mart," *Forbes*, last modified May 24, 2017, accessed January 15, 2018, https://www.forbes.com/sites/laurengensler/2017/05/24/the-worlds-largest-retailers-2017-walmart-cvs-amazon/.

[120] Jeff Dunn, "The Tech Industry Is Dominated by 5 Big Companies — Here's How Each Makes Its Money," *Business Insider Italia*, May 29, 2017, accessed January 15, 2018, http://www.businessinsider.com/how-google-apple-facebook-amazon-microsoft-make-money-chart-2017-5.

[121] Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* (Information Technology and Innovation Foundation, 2017), 5, accessed January 1, 2018, http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.188877538.836303334.1505916541-133641866.1498770015.

[122] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 24.

[123] Courtney M. Bowman, "Data Localization Laws: An Emerging Global Trend," *JURIST*, last modified January 6, 2017, accessed January 18, 2018, http://www.jurist.org/hotline/2017/01/Courtney-Bowman-data-localization.php.

barriers aimed at supporting domestic economy by eroding the US growing monopoly in the tech sector.[124]

In Germany, for example, data localization offers significant economic benefits to Deutsche Telekom, which, indeed, has been lobbied for national localization proposals.[125] As some commentators have argued, "[t]he Snowden revelations have offered a chance for European technology firms to compete against their larger American rivals. Companies like the German telecom giant Deutsche Telekom offer cloud computing services and have tried to use their European roots to lure potential clients away from American competitors".[126] Similarly, the Indian government has long tried to nurture its own IT sector and, not by chance, in the aftermath of Snowden's leaks, the Internet Service Providers Association of India urged the government to enforce data localization measures so as to compete on an even playing field with foreign Net companies.[127] The Guidelines for Nigerian Content Development in Information and Communication Technology (ICT)[128] developed by the Nigeria's National Information Technology Development Agency, and that came into effect in 2013, also exemplify how data localization obligations can be used to promote the local technology sector at the expense of foreign players.[129] These Guidelines prescribe, among other things, that ICT companies shall "[h]ost all subscriber and consumer data locally within the

[124] Millard, *Legal Protection of Computer Programs and Data*, 215–216. See also John M. Eger, "Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers," *Law and Policy in International Business* 10 (1978): 1055–1103.

[125] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 23.

[126] Mark Scott and Nick Wingfield, "Microsoft Suggests Wider Options for Foreign Data," *Bits Blog, The New York Times*, January 23, 2014, accessed January 20, 2018, https://bits.blogs.nytimes.com/2014/01/23/microsoft-suggests-wider-options-for-foreign-data/?mtrref=www.google.co.uk&gwh=8445EBC1CBAF8943DD76801BB17A3EE7&gwt=pay.

[127] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 23–24. See also, Thomas K. Thomas, "Indian Net Firms Want Google, Facebook to Go 'Local,'" *The Hindu Business Line*, last modified June 8, 2013, accessed January 22, 2018, http://www.thehindubusinessline.com/info-tech/indian-net-firms-want-google-facebook-to-go-local/article4795367.ece.

[128] *Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)*, 2013, accessed January 18, 2018, https://nlipw.com/wp-content/uploads/Guidelines-for-Nigerian-Content-Development-in-Information-and-Communications-Technology-ICT.pdf.

[129] Information Technology Industry Council, *ITI Forced Localization Strategy Briefs*, 2016, 8, accessed January 18, 2018, https://www.itic.org/public-policy/ITIForcedLocalizationStrategyBriefs.pdf.

country"[130] and "[h]ost their websites on.ng TLD",[131] i.e., the Internet country code top-level domain for Nigeria. Notably, the stated purpose of the Guidelines is to:

> 1. Enable the local ICT industry to contribute meaningfully towards the achievement of *national development* targets.
> 2. Stimulate and increase the production, sales and consumption of high quality information technology products and services developed by *indigenous companies* that serve the unique needs of the local and global market.
> 3. Enable indigenous information technology companies and provide them opportunities that will *improve* their *ability* to provide relevant products and services that amply satisfy the Nigerian consumer.
> 4. Facilitate efforts to build capacity and equip Nigerians to serve as *active workers* and *participants* in the local ICT industry.
> 5. Provide a framework for the regulation and legislation on the creation, distribution and use of Information Technology and its associations within Nigeria.
> 6. Promote and encourage an environment within Nigeria that is welcoming to *foreign Investments* in Information and Communications Technology, as well as the export of indigenously made ICT goods and services.[132]

On a different note, some argued that data localization measures may be deployed by authoritarian or semi-authoritarian regimes as a means to exert their political control over their population, and hence as a means to stifle political dissent, limit free expression and repress fundamental rights advocates.[133] By way of example, the fact that the Vietnamese data localization law adopted in 2013 (Decree 72/2013) prescribes that international Internet service providers keep "at least one server system in Vietnam serving the inspection, storage, and provision of information at the request of competent state management agencies"[134] reveals the not-so-much covert intent of using data localization for enforcing information control.[135] As clearly stated by Chander and Lê (2015), the underpinning goal of Vietnam's data localization requirements "is not in protecting the privacy of the information from foreign surveillance but in ensuring that information is available to

[130] *Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)*, paragraph 12.1.

[131] Ibid.

[132] Ibid., paragraph 5.0, italics mine.

[133] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 26–27.

[134] Articles 24(2), 25(8), 28(2), *Decree No. 72/2013/ND-CP on Management, Provision and Use of Internet Services and Online Information*, 2013, accessed February 21, 2018, https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF.

[135] Erica Fraser, "Data Localisation and the Balkanisation of the Internet," *SCRIPTed* 13, no. 3 (December 2016): 366, accessed December 30, 2017, https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/.

local authorities that want ready access to it".[136] Similarly, Phil Robertson of Human Rights Watch claimed that Decree 72/2013 is "a law that will be used against certain people who have become a thorn in the side of the authorities in Hanoi".[137] The attempts of the Vietnamese governments to retain control over its citizens' data is further confirmed by a new Cybersecurity law which was adopted by the Vietnamese National Assembly in June 2018 and which entered into force in January 2019. Indeed, the new Cybersecurity law prescribes that both foreign and domestic online service providers shall store the personal data of Vietnamese end-users in Vietnam for a specific period of time and hand those data over to the Vietnamese government authorities upon their request.[138]

By the same token, bearing in mind previous censorship efforts brought forward by the Iranian government, the 2011 proposal for an Iranian "Halal" Internet may just be a mask to disguise its real intent to stifle political opposition and interrupt international communication.[139] This state-sponsored Internet can hence be seen as "another ploy by the Iranian state to limit the spread of information into and around Iran".[140] Similar concerns sparked from the Russian Federal Law No 242-FZ,[141] which was adopted in 2014 (and became effective on 1 September 2015) and requires Internet companies to store data about Russian citizens on servers located within the Russian borders, and from the Cybersecurity Law of the People's Republic of China of 7 November 2016,[142] which became

[136] Chander and Lê, "Data Nationalism," 705.

[137] Quoted in William Gallo and Tra Mi, "New Vietnam Law Bans News Stories From Social Media Sites," *VOA News*, last modified August 2, 2013, accessed January 2, 2018, https://www.voanews.com/a/new-vietnam-law-bans-news-stories-from-social-media-sites/1722190.html.

[138] Jeff Olson, Eddie O'shea, and Mai Phuong Nguyen, "Update: Vietnam's New Cybersecurity Law," *HL Chronicle of Data Protection*, last modified November 15, 2018, accessed October 27, 2019, https://www.hldataprotection.com/2018/11/articles/international-eu-privacy/update-vietnams-new-cybersecurity-law/; Jeff Olson and Mai Phuong Nguyen, "Vietnam Quick to Enforce New Cybersecurity Law," *HL Chronicle of Data Protection*, last modified March 6, 2019, accessed October 27, 2019, https://www.hldataprotection.com/2019/03/articles/international-eu-privacy/vietnam-quick-to-enforce-new-cybersecurity-law/.

[139] Jillian C. York, "Is Iran's Halal Internet Possible?," *Aljazeera*, last modified October 2, 2012, accessed January 2, 2018, http://www.aljazeera.com/indepth/opinion/2012/10/201210263735487349.html.

[140] Katie Beiter, "Iran Introduces Halal Internet," *The Media Line*, September 8, 2016, accessed January 2, 2018, http://www.themedialine.org/news/iran-introduces-halal-internet/.

[141] *Federal Law No. 242-FZ on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks*, 2014, accessed February 21, 2018, https://pd.rkn.gov.ru/authority/p146/p191/.

[142] *Cybersecurity Law of the People's Republic of China, 24th Session of the Standing Committee of the 12th National People's Congress*, 2016.

effective on 1 June 2017 and prescribes that all users' personal information and important data collected and produced by critical information infrastructures operators during their activities within the People's Republic of China shall be stored in mainland China. In the light of the above, it has been argued that transborder data flow, rather than exposing data to extra risks, may enhance protection of personal data by placing them beyond the control of authoritarian authorities.[143]

Moreover, even in places or in circumstances where data localization is not prescribed as a binding legal requirement, public demand has played an important role in encouraging companies to establish in-country data centres. People are more and more concerned about the vulnerability of their personal data, thus making location of data centres an important purchasing consideration.[144] Google's decision to add a new option to its privacy policy that allows its customers to choose to store their data in Europe "in response to popular demand",[145] seems instructive in this respect. Similarly, in 2015, Apple announced its plan to invest € 1.7 billion to build new data centres in Europe[146] and, according to some, this move is "likely to comfort European politicians and security industry insiders who have criticized the U.S. National Security Agency for poring over European citizens' data held in U.S. facilities".[147] In the aftermath of Snowden's revelations, Amazon has also announced its intention to build new data centres in Germany in order to address European concerns.[148] Similarly, Jottacloud, a Norwegian cloud storage service that allows its customers to

[143] Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, 6.

[144] "Meeting the Challenge of Data Localization Laws." Dockery also noted that keeping data within a specific country can "put consumers at ease about government surveillance". Stephen Dockery, "Data Localization Takes Off as Regulation Uncertainty Continues," *The Wall Street Journal*, June 6, 2016, accessed November 2, 2019, https://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/.

[145] Navneet Joneja, "Google Storage for Developers Open to All, with New Features," *Google Developers Blog*, May 10, 2011, accessed January 19, 2018, https://developers.googleblog.com/2011/05/google-storage-for-developers-open-to.html.

[146] "Apple to Invest €1.7 Billion in New European Data Centres," *Apple Newsroom*, last modified February 23, 2015, accessed January 20, 2018, https://www.apple.com/newsroom/2015/02/23Apple-to-Invest-1-7-Billion-in-New-European-Data-Centres/.

[147] David Lumb, "Why Apple Is Spending $1.9 Billion To Open Data Centers In Denmark And Ireland," *Fast Company*, last modified February 23, 2015, accessed January 20, 2018, https://www.fastcompany.com/3042746/why-apple-is-spending-19-billion-to-open-data-centers-in-denmark-and-ireland.

[148] Murad Ahmed, "Amazon to Open German Data Centres to Soothe European Concerns," *Financial Times*, last modified October 23, 2014, accessed February 16, 2018, https://www.ft.com/content/56181a6e-5a96-11e4-b449-00144feab7de.

back up, store and share files over the Internet, committed to store all files in Norway, or in "a country with similar or stricter privacy laws", so as to protect its users "against U.S. legislation, which arguably infringe the freedom and liberties of both U.S and non-U.S. citizens".[149] In 2014, Microsoft's decision to take steps to increase its users' ability to make an informed choice about the location of their data has been at least partly driven by the need to regain users' trust after Snowden's leaks.[150] In the wake of the Snowden revelations, other companies, such as Facebook, IBM, and Amazon.com also announced their plans to build new data centres to protect their customers' data from US snooping.[151]

As a further confirmation of this trend, a 2015 KPMG study on cloud computing in Germany found that, following the NSA incident, 83% of the customers surveyed expects cloud providers to have their computer centres and headquarters in Germany, or at least within the EU area.[152] In addition, a 2014 NTT Communications study on ICT decision-makers' approach to cloud from France, Germany, Hong Kong, the USA and the UK has found that companies are taking action for keeping data where "they know it will be safe", even if these actions may come at the expense of a swift development of cloud computing projects and, in turn, at the expense of performance gains.[153] In particular, the survey found that, when it comes to data storage in the cloud, 30% of the ICT decision-makers surveyed in Germany and in the US, 24% of those surveyed in France and Hong Kong, and 22% of the decision-makers surveyed in the UK agreed that "location completely matters".[154] Such pressures from the public as well as from domestic ICT companies have led to what

[149] Roland Rabben, "It's Your Stuff — Guaranteed!," *Jottacloud*, last modified June 16, 2013, accessed January 20, 2018, https://blog.jottacloud.com/its-your-stuff-guaranteed-3f50359f72d.

[150] Scott and Wingfield, "Microsoft Suggests Wider Options for Foreign Data." See also "Where Your Data Is Located," *Microsoft Trust Center*, accessed January 20, 2018, https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located.

[151] "Meeting the Challenge of Data Localization Laws." See also, Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *The New York Times*, March 21, 2014, accessed January 20, 2018, https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

[152] KPMG, *Cloud Monitor 2015 Cloud Computing in Germany. Status Quo and Perspectives*, 2015, 5–32.

[153] NTT Communications, *NSA After-Shocks. How Snowden Has Changed ICT Decision-Makers' Approach to the Cloud*, 2014, 1, accessed January 20, 2018, http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf.

[154] Ibid., 3.

Kuner (2015) has described as a "chicken or egg" dilemma: "did governments initiate [data localization measures] to benefit domestic interests, or was it domestic pressures from business and individuals that led to governments becoming interested in the topic?".[155]

Overall, data localization measures, in their diverse manifestations, have now achieved a global reach. The Russian Federation and People's Republic of China have adopted the most extended and commented-on forms of data localization. Other countries have adopted sector-specific measures, i.e., measures tailored to some specific datasets or to some specific industry sectors. By way of example, in Australia, under certain circumstances, personally identifiable health records cannot leave the Australian territory;[156] in Switzerland, banking and financial regulations may require in-country data storage;[157] two Canadian provinces mandate that personal data held by some public bodies, such as schools and hospitals, are stored and accessed domestically;[158] in South Korea, mapping data cannot be stored offshore for security reasons;[159] in 2018, the Reserve Bank of India has mandated that payment service providers store all payment data in India "in order to ensure better monitoring".[160]

Leaving aside explicit data localization requirements, some States have adopted provisions that may *de facto* lead to in-country data storage. The European Union, by making data transfer to third parties conditional upon the compliance with strict requirements, may effectively induce companies towards in-country data storage and processing.[161] Likewise, the Law on the Protection of Personal Data adopted in Turkey in 2016 may translate into a data localization requirement since data controllers and processors cannot transfer personal data to third countries without the express consent

---

[155] Kuner, "Data Nationalism and Its Discontents," 2095.

[156] Drake, Cerf, and Kleinwächter, *Internet Fragmentation: An Overview*, 44.

[157] Ibid. See also Stéphanie Chuffart-Finsterwald, "Data Protection in Switzerland: Overview," *Practical Law*, last modified July 1, 2016, accessed January 18, 2018, https://uk.practicallaw.thomsonreuters.com/9-502-5369?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

[158] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 21.

[159] Drake, Cerf, and Kleinwächter, *Internet Fragmentation: An Overview*, 44. See also, Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 28.

[160] See the notification of the Reserve Bank of India, available at https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

[161] Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, 5.

of the individuals concerned.[162] Whichever form these measures have taken or may take, States' effort of keeping (certain types of) data within their national borders witnesses how, despite the "un-territoriality of data"[163] and the globalized and interdependent nature of modern economy, geography still retains a great deal of importance.[164]

2.4. From Internet to "Splinternet": What Are the Drawbacks?

The existing literature has by-and-large addressed the recent global spread of data localization measures by highlighting its allegedly inner inconsistencies and fallacies. Firstly, by drawing borders in a borderless domain, data localization is deemed to challenge the "very nature of the World Wide Web".[165] Indeed, the Internet was essentially designed to allow the sharing and the flow of information regardless of traditional geographic and political borders and Internet users are often unaware of where their data are physically stored. As a result of the long-standing tensions between national sovereignty and transnational Internet,[166] data localization may cause an unwarranted fragmentation of the unified and flexible nature of the Internet by dividing the "global public Internet" into "bordered national Internets".[167] "Splinternet" is hence emerging as a substitute for Internet.[168]

Moreover, by placing bottlenecks on the routes along which data flow, restricted routing would also greatly affect the way Internet works: data will no longer follow the traditional "best effort

[162] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 29. See also Yusuf Mansur Özer, "GDPR Matchup: Turkey's Data Protection Law," August 10, 2017, accessed October 27, 2019, https://iapp.org/news/a/gdpr-matchup-turkeys-data-protection-law/.

[163] Jennifer Daskal, "The Un-Territoriality of Data," *The Yale Law Journal* 125 (2015): 326–398, accessed January 31, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2578229.

[164] Christopher Millard, "Forced Localization of Cloud Services: Is Privacy the Real Driver?," *IEEE Cloud Computing* 2, no. 2 (April 2015): 13.

[165] Chander and Lê, "Data Nationalism," 680.

[166] Drake, Cerf, and Kleinwächter, *Internet Fragmentation: An Overview*, 9.

[167] Ibid., 5. Drake et al. identify three forms of Internet fragmentation. Firstly, technical fragmentation that indicates "conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points"; secondly, governmental fragmentation that includes "[g]overnment policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources"; thirdly, commercial fragmentation that is a label for "[b]usiness practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources". Data localization measures fall under governmental fragmentation. Ibid., 4.

[168] John Ribeiro, "At Senate hearing, Google warns of 'splinternet' but NSA does not budge", *PCWorld*, November 14, 2013, accessed October 4, 2017, https://www.pcworld.com/article/2063520/at-senate-hearing-google-warns-of-splinternet-but-nsa-does-not-budge.html. See also, Michael Hayden, "Is Internet in danger of becoming 'splinternet'?", *CNN*, February 14, 2014, accessed October 4, 2017, http://edition.cnn.com/2014/02/14/opinion/hayden-splinternet-snowden/index.html.

delivery model", according to which data are sent to their destination through the most direct possible way, but will follow predetermined paths so as to prevent data from moving through "prohibited" territory. Such alterations would require a major restructuring not only of Internet infrastructures but also of its governance mechanisms.[169] As stated by Richard Salgado, Google's director of law enforcement and information security, before the Senate Judiciary Subcommittee on Privacy, Technology, and the Law in November 2013, "[i]f data localization and other efforts are successful, then what we will face is the effective Balkanization of the Internet and the creation of a 'splinternet' broken up into smaller national and regional pieces, with barriers around each of the splintered Internets to replace the global Internet we know today".[170]

Moreover, it has been argued that information security and privacy are not well-served by data localization measures. Data location is not a function of security:[171] "[d]ata breaches can and do occur anywhere".[172] As Bildt (2015) has noted, "[t]he solution to privacy concerns lies not in data localization but in the development of secure systems and the proper use of encryption. Data storage actually means the continuous transfer of data between users, with no regard for Westphalian borders".[173] Data security is hence dependent on the effectiveness and on the quality of the security measures implemented by Internet service companies for protecting the data they hold[174] rather than on geography. Moreover, large-scale cloud computing providers are likely to ensure better security than local alternatives. Indeed, the implementation of advanced security measures requires capital and highly qualified personnel, which is precisely what small and medium-sized companies struggle

[169] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 33–34.

[170] Richard Salgado, "Written Testimony before the Senate Judiciary Subcommittee on Privacy, Technology and the Law," November 13, 2013, 3, accessed January 20, 2018, http://services.google.com/fh/files/blogs/google_testimony_transparency_nov132013.pdf.

[171] Matthias Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery* (ECIPE occasional paper No. 3/2014, 2014), 3, accessed February 11, 2019, https://ecipe.org/publications/dataloc/.

[172] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 29.

[173] Carl Bildt, "One Net, One Future," *Centre for International Governance Innovation*, last modified October 26, 2015, accessed January 26, 2018, https://www.cigionline.org/articles/one-net-one-future.

[174] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 29. See also, W. Kuan Hon et al., "Policy, Legal and Regulatory Implications of a Europe-Only Cloud," 13.

to provide and which large organizations can offer.[175] The conclusion of a 2015 Leviathan Security study commissioned by Google seems to be instructive in this respect. The study noted that the cybersecurity arena suffers from employee scarcity, i.e., the difficulty that employers encounter in recruiting highly qualified security experts. Several cybersecurity positions worldwide are unfilled due to talent and education shortages and the few security experts available tend to gather in large organizations: "[a]ny plan that requires a country to source locally its security talent, its data, or its computational infrastructure may be requiring the impossible".[176]

Moreover, with specific reference to counter-surveillance objectives, it has been noted that in the absence of adequate security measures, in-country data storage does not prevent foreign authorities from gathering data via *remote* access.[177] Some even argue that data localization may facilitate rather than limit foreign surveillance by causing the so-called "jackpot" problem: information assembled in one place certainly represents a tempting "jackpot" for illegitimate governmental and nongovernmental activities.[178] Indeed, the centralization of data in one specific region allows foreign agencies to focus their surveillance efforts in one area rather than in multiple places, thus easing their logistical burdens.[179]

---

[175] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 4.

[176] Leviathan Security Group, *Analysis of Cloud vs. Local Storage: Capabilities, Opportunities, Challenges*, 2015, 7, accessed January 20, 2018, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dada7e4b069728afca39b/1436396967533/Value+of+Cloud+Security+-+Scarcity.pdf. In another study, the Leviathan Security Group also found that by taking advantage of geographical redundancy, cloud services provide greater resiliency than local services in the face of local or regional incidents of any sort (e.g., the data meltdown in Calgary caused by an explosion in 2012, the damages that Hurricane Sandy caused to data centres hosted in New York in 2012, and the damages caused to many undersea cables in Japan by the 2011 Tohoku earth- quake). Indeed, by replicating data worldwide, cloud storage secures data availability and survivability when local datacentres fail: "[t]he capability exists to make data storage, not just communication, resilient in the face of large-scale threats; it requires only that companies and governments not restrict communications on the basis of geographic boundaries". Leviathan Security Group, *Comparison of Availability Between Local and Cloud Storage*, 2015, 14, accessed January 22, 2018, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad9ae4b069728afca34a/1436396954508/Value+of+Cloud+Security+-+Availability.pdf.

[177] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 29.

[178] Chander and Lê, "Data Nationalism," 719.

[179] Ibid., 717. See also, Martina Francesca Ferracane, "How Data Localisation Wipes out the Security of Your Data," *Security Europe*, n.d., accessed February 16, 2018, http://www.securityeurope.info/how-data-localisation-wipes-out-the-security-of-your-data/.

Moreover, policymakers advancing data localization also disregard another important factor: foreign authorities may still gain access to data from domestic authorities, who can easily access such data and, in the spirit of mutual cooperation, decide to pass those data – formally or informally – to their foreign counterparts. After all, no one has ever said that law enforcement authorities should never have access to data held in foreign soils, simply that these data should not be accessed by way of illegitimate and indiscriminate spying.[180] But even admitting that data localization may reduce the risk that data fall in *foreign* hands, in-country data storage surely gives greater power to *domestic* intelligence agencies and governments. As Hill (2014) has put it, since "it is those domestic agencies and their governments, and not the NSA and the United States, that can more immediately impose and enforce coercive measures upon the citizens, those citizens need to ask themselves ... which presents the greater threat to their liberty generally, and to the security of their personal information in particular?".[181]

Great concerns have also been voiced with reference to the impact that data localization may have on freedom of expression. Data localization may, indeed, be deployed as a form of information control, and information control is an essential component of authoritarian regimes which routinely target and suppress adverse information. The Internet should be applauded for having made this control more difficult.[182] Thanks to its free and essentially ubiquitous nature, the Internet allows people to engage in information exchange without geographical limitations; it has fostered individuals' active participation in political decision-making processes and has become an essential instrument for advancing democracy and human rights protection. However, data localization measures may severely infringe upon Internet's potentials in supporting freedom of expression by making Internet users more exposed to governments' control.[183] By bringing information under

[180] Hon et al., *Policy, Legal and Regulatory Implications of a Europe-Only Cloud*, 17.

[181] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 30.

[182] Chander and Lê, "Data Nationalism," 735.

[183] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 33.

national jurisdiction, and therefore under national control, data localization helps domestic public authorities monitor Internet platforms so as to avoid political unrest,[184] idendify the authors of allegedly subversive comments, and, eventually, prosecute them. As Hill (2014) has put it, data localization and the consequent alteration in the Internet's operating structures would give governments a "previously unavailable capacity to assess where data had originated and where it was heading because the origin and destination information would be included in the data packet".[185]

The intent to promote and stimulate local economies is also misplaced according to many. Firstly, preventing foreign companies from operating within a country, or making their operations more burdensome would result in fewer options readily available to local customers. Local customers also include small businesses which would hence be precluded from benefiting from more affordable and more technologically advanced services that only big international corporations and their economies of scale can furnish.[186] In the words of Chander and Lê (2015), "data localization raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and interferes with the use of the latest technological advances".[187] Secondly, job opportunities that revolve around the construction of new data centres are limited in number. Indeed, since data servers farms are becoming more and more automated, the high number of temporary construction jobs is not followed by an equally high number of full-time jobs:[188] "[t]he data centers that power the cloud and run programs such as Gmail and iTunes employ thousands of servers but only dozens of people".[189] The property tax benefits that supposedly derive from data localization are equally likely

[184] Ibid., 26–27.

[185] Ibid., 34.

[186] Ibid., 31. See also a 2015 Leviathan study which quantified the harms that laws limiting cross-border data flow cause to individuals and businesses when they are mandated to use exclusively local data centres, Leviathan Security Group, *Quantifying the Cost of Forced Localization*, 2015, accessed January 24, 2018, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

[187] Chander and Lê, "Data Nationalism," 721.

[188] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 5. See also, Selby, "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?," 229.

[189] Michael S. Rosenwald, "Cloud Centers Bring High-Tech Flash but Not Many Jobs to Beaten-down Towns," *The Washington Post*, November 24, 2011, accessed January 22, 2017, https://www.washingtonpost.com/business/economy/cloud-centers-bring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html?utm_term=.6b1093c1893c.

to be outweighed by the financial incentives that local governments would need to award in order to lure big companies to locate their data centres in their soil.[190] Moreover, since data farms require a large amount of energy, data localization may further increase the demand, and hence the price, of an already overtaxed power.[191]

Similarly, the allure of increasing local investments by mandating (or inducing) companies to localize data within national borders will probably be unsatisfied. Indeed, the adoption of data localization measures often places companies before a binary choice: either comply with data localization requirements or abandon those markets.[192] When faced with a similar situation, some companies may lack the economic as well as the human resources to make the necessary arrangements for complying with complex data localization requirements.[193] Compliance with data localization provisions is, indeed, expensive[194] since it requires companies to spend more on data-storage services and on compliance activities. In particular, the largest cost that companies may need to bear derives from the investments required for building new in-country data centres.[195]

Back in 1981, Jane Bortnick commented on the possible impact on corporations of the cross-border data flow regulation implemented in Brazil, by stating that

> [a] multinational corporation desiring to operate in Brazil, ..., may be forced to establish *duplicate* data processing facilities in Brazil rather than receive services or equipment directly from abroad. Consequently, the cost of doing business may drastically increase. Furthermore, the unavailability of adequate equipment and services produced in Brazil may lead to *less efficient* operations ... Finally, the increase in cost and decrease in efficiency may simply *preclude* an enterprise *from entering* a market such as Brazil.[196]

---

[190] Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, 7.

[191] Chander and Lê, "Data Nationalism," 724–725.

[192] Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, 4.

[193] Bowman, "Data Localization Laws: An Emerging Global Trend."

[194] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 6–7. These costs will inevitably translate into either a decrease in profit margins for the firms or in higher prices for their customers. On the inefficiencies that may derive from barriers to data flow see also The Business Roundtable, *Putting Data to Work: Maximizing the Value of Information in an Interconnected World*, 2015, 25–32, accessed February 7, 2018, http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf.

[195] The Business Roundtable, *Putting Data to Work: Maximizing the Value of Information in an Interconnected World*, 28.

[196] Bortnick, "International Information Flow: The Developing World Perspective," 343 (italics mine).

Almost forty years later, Cohen et al. (2017) noted that

> [a] rising trend in forced data localization measures could result in companies either *avoiding* certain markets altogether or being forced to create and maintain *numerous* data centers. Such measures may hinder a firm's ability to exercise business judgment in managing its business risks and needs, reduce opportunities to take advantage of global economies of scale and expertise that may benefit privacy and security...[197]

Small and medium sized companies are likely to be the most affected by data localization measures. Indeed, as it is clearly stated in a 2016 study of the European Centre for International Political Economy (ECIPE): "Small and Medium Sized Enterprises (SMEs) are more vulnerable to costs arising from domestic regulations, as they are less able to adjust their supply chains, human resources or to invest in alternative solutions".[198] Similar concerns have also been expressed by Nicholson and Noonan (2014) when they stated that "[l]ocalization requirements carry great risk of limiting the Internet's global character, making cross-border trade difficult for large companies and practically impossible for small businesses that cannot afford to implement separate systems and standards in every country in which they do business".[199]

Most importantly – or maybe, most alarmingly – in a context where economic growth increasingly relies on "how firms collect, transfer, analyse, and act on data",[200] data localization is deemed to have disruptive effects on economic growth and global development more broadly. Several studies have tried to quantify the economic impact of data localization. In 2013, the ECIPE quantified the potential external trade impact of the GDPR. By translating the costs for complying with EU data protection law in non-tariff barriers and applying these barriers to US companies exporting to the EU,

---

[197] Bret Cohen, Britanie Hall, and Charlie Wood, "Data Localization Laws And Their Impact on Privacy, Data Security And the Global Economy," *Antitrust* 32, no. 1 (2017): 108, accessed February 15, 2018, https://www.perkinscoie.com/en/news-insights/data-localization-laws-and-their-impact-on-privacy-data-security.html.

[198] Matthias Bauer et al., *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States* (ECIPE, Policy Brief No. 03/2016, 2016), 8, accessed November 2, 2019, https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/.

[199] Jessica R. Nicholson and Ryan Noonan, *Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services* (ESA Issue Brief # 01-14, United States Department of Commerce: Economics and Statistics Administration, 2014), 8, accessed January 25, 2018, https://www.tralac.org/images/News/Documents/Digital_Economy_and_Cross-Border_Trade_ESA_Issue_Brief_January_2014_US_Department_of_Commerce.pdf. See also, Leslie Harris, "Don't Gerrymander the Internet," *Index on Censorship*, November 4, 2013, accessed February 16, 2018, https://www.indexoncensorship.org/2013/11/dont-gerrymander-internet/.

[200] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 6.

the study found that US service exports to the European Union would decrease by – 0.2% to – 0.5%. Similarly, EU exports to the US would drop by -0.6% to -1% due to loss of competitiveness.[201] The GDPR may hence disrupt the services supply between the EU and its commercial partners, and since "the EU is a major world economy, such disruptions risk affecting the entire global trading system".[202] "The question is whether the conflict between the current political momentum in favor of far-reaching privacy legislation and EU's role as the leading trading bloc can be reconciled".[203] In another study conducted in 2014, the ECIPE quantified the costs deriving from data localization measures with a focus on seven countries (Brazil, China, the European Union, India, Indonesia, South Korea and Vietnam) and concluded that "[a]ny gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy".[204]

In another study conducted in 2016, ECIPE identified 22 data localization measures enacted by EU Member States and aimed at restricting the data flow to other EU Member States. The purpose of the study was to estimate the economic impact if these measures were removed (the "Liberalisation Scenario") and if these measures were strengthened (the "Ratchet Scenario"). The study found that, in the Liberalisation Scenario, the GDP of the Member States examined would increase, for example, by 0.05 percent in the United Kingdom and Sweden, 0.06 % in Finland, 0.07 % in Germany, 0.18 % in Belgium, and 1.1 %in Luxembourg. Overall, the EU GDP would increase by up to 0.06 %.[205] On the other hand, in the Ratchet Scenario, the study found that GDP losses would vary in individual States, ranging from -0.42% in Italy, -0.36% in Spain, -0.30% in the UK, and -0.33% in Germany. As a whole, the study estimated that the EU economy would lose around 0.4% or 52 billion euros every year.[206]

---

[201] Matthias Bauer et al., *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce* (ECIPE, 2013), 12–13, accessed January 24, 2018, https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

[202] Ibid., 8.

[203] Ibid., 9.

[204] Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, 2.

[205] Bauer et al., *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States*, 10 – 11. The GDP gains identified under the Liberalisation Scenario are comparatively low. This derives from the fact that most of the measures implemented are limited in scope.

[206] Ibid., 11–12.

Moreover, small and medium-sized enterprises and developing countries are likely to suffer the most from the harms deriving from data localization measures. According to a study conducted by the Global Economy and Development program at Brookings in 2014, Internet represents an opportunity for SMEs and developing countries for becoming active part of international trade, and hence of global economy. The Internet is, in fact, replete with appealing economic potentials. Among others, it provides SMEs and developing countries with access to new sources of finance, such as crowdfunding, it gives them access to information about foreign markets that can help them expand overseas, and it allows them to trade goods online thus bypassing the need to establish offices in the countries where they export.[207] Against this background, restrictions to cross-border data flow severely limit Internet capability of serving as a platform for engaging in international trade, and consequentially contribute to the isolation of weaker actors from major global markets.[208] Ezell et al. (2013) expressed a similar concern in stating that localization barriers to trade – that also include restrictions on data flow — weakens local companies' ability to become part of global economy by raising their costs and by limiting their chance to access technology.[209]

Similar conclusions were reiterated in a 2014 Deloitte study. The Internet fosters economic growth in a host of ways: it enhances information exchange thus reducing transaction costs, it fosters innovation and facilitate access to financial capital, it supports entrepreneurs by easing their access to new markets, and it improves human capital by offering individuals new "affordable" education opportunities.[210] The study also highlighted that benefits deriving from the Internet should be

[207] Joshua Meltzer, *Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium Sized Enterprises and Developing Countries* (Global Economy and Development Working Paper 69, The Brookings Institution, 2014), 5–8, accessed January 24, 2018, https://www.brookings.edu/wp-content/uploads/2016/07/02-internet-international-trade-meltzer.pdf.

[208] Ibid., vi.

[209] Ezell et al., *Localization Barriers to Trade: Threat to the Global Innovation Economy*, 47.

[210] Deloitte, *Value of Connectivity: Economic and Social Benefits of Expanding Internet Access*, 2014, 3, accessed January 24, 2018, https://www2.deloitte.com/view/en_GB/uk/industries/tmt/extending-internet-access/index.html. For an analysis of the economic benefits of the Internet and of cross-border data flow see also Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 2–4; GSMA, *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC Can Protect Data and Drive Innovation*, 2018, 68–71, accessed November 1, 2019, https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.

measured not only in economic but also in social terms. Indeed, the Internet leads to health improvements by broadening access to medical information and by providing doctors with new medical devices to treat and monitor their patients;[211] it "unlocks universal education" by giving teachers and students access to new and up-to-date learning resources;[212] it favours social inclusion by strengthening the connections between community members and by providing individuals with new tools, such as social networks, for becoming actively involved in the social and political arena.[213] All in all, "if developing countries could bridge the gap in internet penetration to reach levels developed economies enjoy today, they would experience large increases in GDP growth and productivity and improvements in health conditions and education opportunities".[214]

Data localization may also impair innovation as well as access to innovation. Indeed, data localization restricts not only the flow of data but also the ideas and the new technologies that flow along with data.[215] In a context where data are an essential ingredient for creating new products and services, data localization prevent companies from taking advantage of the ideas and innovative technologies that rely on data. As a result, companies that operate in countries that have implemented data localization measures would hardly be as innovative as the companies that operate in global markets without similar constraints, or they would need to bear higher costs for reaching the same level of innovation.[216] According to a 2012 study of Business Roundtable, "[w]hen trade barriers disrupt the free flow of lawful information, they can result in a slowing of technological innovation and prevent companies from offering certain products and services, consequently dampening economic growth".[217]

---

[211] Deloitte, *Value of Connectivity: Economic and Social Benefits of Expanding Internet Access*, 4.

[212] Ibid., 5.

[213] Ibid., 6. On the social benefits of Internet openness see also, Organisation for Economic Cooperation and Development, *Economic and Social Benefits of Internet Openness* (Paris: OECD Digital Economy Papers No. 257, OECD Publishing, 2016), 46–49, accessed February 16, 2018, http://www.oecd-ilibrary.org/docserver/download/5jlwqf2r97g5-en.pdf?expires=1519237452&id=id&accname=guest&checksum=F97665039CC2F5EC59376BE4F8E314D7.

[214] Deloitte, *Value of Connectivity: Economic and Social Benefits of Expanding Internet Access*, 2.

[215] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 7.

[216] Ibid.

[217] Business Roundtable, *Promoting Economic Growth through Smart Global Information Technology Policy. The Growing Threat of Local Data Server Requirements*, 2012, 4, accessed January 25, 2018, http://businessroundtable.org/sites/default/files/Global_IT_Policy_Paper_final.pdf.

By the same token, when data localization measures are in place, fruitful cooperation between firms, research organizations and universities could be impaired since such cooperation inevitably leads data to move across borders.[218] The Internet, in fact, plays an essential role in stimulating innovation by providing researchers, academics and firms with essential platforms for exchanging their knowledge on a global scale.[219] Barriers to knowledge sharing may, for example, severely hamper advances in medical research. The development of cures, indeed, heavily relies on the creation of large and shared datasets: "disease does not stop at national borders, meaning that data needed to find cures need to cross borders, too".[220] This entails that barriers to data flow not only undermine research and innovation but also preclude citizens from having access to the most-sophisticated medical services and technological advances more broadly.[221] More generally, data localization reduces Internet's capacity for productivity by reducing its network effect. As Hill (2014) has stated, by excluding some companies from the network, "data localization reduces the overall size of the network, which, according to network theory as well as Metcalfe's Law (which states that the value of a communications network is proportional to the number of users of the system), would bring up both costs and the overall innovative potential of the aggregated network".[222]

From a more general perspective, Internet access can be considered as a human right *per se* and any restrictions to it that may derive from data localization a violation of this right.[223] A 2011 survey of 5,400 Internet users from 13 countries revealed that 72% of the respondents agreed that Internet access should be considered as a fundamental right. Interestingly, the highest proportions were found in countries with the lowest Internet diffusion rates among which Mexico (82%), South

[218] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 7.

[219] Sarah Box, *Internet Openness and Fragmentation: Toward Measuring the Economic Effects* (Global Commission on Internet Governance, Paper Series No. 36, 2016), 2–3, accessed January 25, 2018, https://www.cigionline.org/sites/default/files/gcig_no.36_web.pdf.

[220] Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 7.

[221] Ibid., 8.

[222] Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," 32.

[223] Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 9–10.

Africa (81%), and India (77%).[224] In 2016, this view has been formally cemented in a UN resolution in which the UN Human Rights Council affirmed "the importance of applying a human rights-based approach in providing and in expanding access to Internet"[225] and condemned measures that "intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law".[226] Not by chance, a minority of States rejected this resolutions, among which Russia and China.[227]

2.5. Conclusion

Data localization is widely perceived as an "emerging global trend".[228] The analysis conducted in this chapter has shown that several States have implemented policies aimed at directly or indirectly control data entering and leaving their borders. As seen above, data localization includes different *types* of policies like localized data hosting, localized data routing, policies that require that data are processed by companies in specific jurisdictions, policies that select companies that can handle data on the basis of their nation of incorporation, and policies that restrict transborder data flow. The adoption of such policies may be motivated by different reasons that scholars have attempted to unveil. Privacy and information security are often mentioned as triggers of data localization: the fear is that the data protection standards that States offer to individuals may be eroded once data are transferred to States which do not offer the same level of protection. After Snowden's

[224] Soumitra Dutta, William H. Dutton, and Ginette Law, *The New Internet World, A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online* (INSEAD Working Paper No. 2011/89/TOM, 2011), 9, accessed January 29, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1916005.

[225] United Nations Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet, 32nd Session* (A/HRC/32/L.20, 2016), 3, accessed January 2, 2019, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

[226] Ibid., 4.

[227] Among others, Emma Boyle, "UN Declares Online Freedom to Be a Human Right That Must Be Protected," *The Independent*, last modified July 5, 2016, accessed January 26, 2018, http://www.independent.co.uk/life-style/gadgets-and-tech/un-declares-online-freedom-to-be-a-human-right-that-must-be-protected-a7120186.html; "United Nations Declares Internet Access a Human Right; Cuba, Venezuela Oppose Move," *Fox News*, last modified July 6, 2016, accessed January 26, 2018, http://www.foxnews.com/politics/2016/07/06/un-resolution-declares-internet-access-human-right-cuba-venezuela-oppose-it.html; Catherine Howell and Darrell M. West, "The Internet as a Human Right," *Brookings*, November 7, 2016, accessed January 26, 2018, https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/; James Vincent, "UN Condemns Internet Access Disruption as a Human Rights Violation," *The Verge*, last modified July 4, 2016, accessed January 26, 2018, https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access.

[228] Bowman, "Data Localization Laws: An Emerging Global Trend."

revelations, data localization measures also started to be implemented in the attempt of shielding data from foreign intelligence agencies. Some even argued that instead of protecting data from foreign public authorities, data localization measures are meant to support domestic intelligence and law enforcement authorities in gaining easier access to their citizens' data. Protectionism and the intent to favour the domestic information technology sector at the expenses of foreign, mainly US, technology giants have also been identified by some scholars as another possible trigger of data localization measures. As seen in this chapter, there are strong reasons to believe that data localization measures may also be implemented by authoritarian or semi-authoritarian regimes as a means to exert their political control over their population.

The adoption of (forced) data localization measures has hence emerged as a global trend. At the same time, the specificities of the national or regional legal provisions that underpin such measures should not be neglected since such specificities often mirror their surrounding legal and political framework. This trend shows that both governments and cloud/Internet users attach a great deal of importance to data location even if restricting data movement may come at the expenses of economic efficiencies (and global development more broadly) and even if the effectiveness of such measures in achieving their underpinning goals has been widely questioned. As highlighted above, the European Union is part of this trend since both the 1995 Directive and the GDPR set out some specific rules which regulate, and consequently restrict, international data flow. The next chapter will start delving into the EU data protection framework of which data transfer restrictions are an essential component. The analysis of the GDPR will start from one of the first, and yet most controversial provision of the Regulation, i.e., the territorial scope of the Regulation as defined under Article 3. A clear understanding of the breadth of the territorial scope of the GDPR will prove essential to understand how and to what extent the rules on the territorial scope of the Regulation and the rules on international data transfer, and their underlying objectives, interact and overlap.

3. The (Extra)Territorial Scope of the General Data Protection Regulation

3.1. Introduction

A clear understanding of the territorial scope of the GDPR is essential to ensure legal certainty for individuals and other stakeholders, both in the European Economic Area and in the wider international framework. Indeed, from the perspective of the data subject, and hence from a fundamental rights perspective, clear rules on applicable law guarantee that no lacunae and inconsistencies arise in the EU data protection framework. Moreover, legal certainty is essential for companies that engage in cross-border activities since it determines when the data protection rules set out in the Regulation apply to them in the first place. Yet, little clarity has been shed, and can be shed, on the exact breadth of the territorial scope of the Regulation and on its possible practical implications, especially considering that some processing activities carried out by a controller or a processor might fall under the GDPR while other processing activities by the same controller or processor might fall outside the scope of the Regulation.[229] The draft Guidelines[230] that have been adopted in November 2018 by the EDPB on the territorial scope of the GDPR have partially clarified the (extra)territorial applicability of the GDPR while leaving several open questions which, unfortunately, have not been completely answered in the final version adopted one year later after the public consultation.

The loopholes in the protection of data subjects and the low degree of predictability of liability for companies that may derive from these uncertainties seem to go against the overall objective of the Regulation, that can be confidently identified in the same objective that, back in 2010, the A29WP

[229] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 2019, 5, accessed December 15, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf.

[230] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version for Public Consultation*, 2018, accessed December 15, 2019, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

attributed to the 1995 Directive:[231] "guaranteeing an effective protection to individuals, in a simple, workable and predictable way".[232] This chapter hence analyses the grounds based on which the Regulation applies with a view to shedding some clarity on their possible interpretation and implications while, at the same time, identifying their weaknesses in addressing many of the key concerns that have been voiced under the 1995 Directive. The experience gained by implementing Article 4 of the DPD, the related case-law, the guidelines and opinions offered by the A29WP and the EDPB, the advances in other contexts of EU law will be the main reference points in this analysis.

3.2. The (Extra)Territorial Scope of the GDPR

3.2.1. From the (Extra)Territorial Scope of the 1995 Directive to the (Extra)Territorial Scope of the GDPR

Many commentators mention the extraterritoriality of the Regulation, and of the 1995 Directive before it, as one of the main features of the EU data protection legislation. However, there is no widely accepted definition of extraterritorial jurisdiction[233] and even when a definition is adopted, drawing a line between territorial jurisdiction and extraterritorial jurisdiction can be highly challenging. A useful definition of extraterritorial jurisdiction is provided by the International Law

[231] "The current framework remains sound as far as its objectives and principles are concerned". European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM(2012) 11 final. (Brussels, 2012), 2, accessed November 24, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.

[232] Article 29 Data Protection Working Party, *Opinion 8/2010 on Applicable Law (WP179)*, 2010, 14, accessed January 2, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf.

[233] As noted in WP179, in data protection law, it is important to distinguish between "applicable law" (i.e., which law applies to a given processing) and "jurisdiction" (i.e., which State or entity has regulatory power over that activity and hence to decide and enforce an order or a judgement). Applicable law and jurisdiction over a specific processing activity do not always coincide (although most of the time they do). By way of example, Article 28(6) of the 1995 Directive prescribes that "[e]ach supervisory authority is competent, *whatever the national law applicable to the processing in question*, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3" (italics mine), such as investigative powers and powers of intervention. Under the Regulation, a similar mismatch between the applicable law and the authority having regulatory power may arise from the one-stop-shop mechanism prescribed under Article 56. However, the relevance of this distinction is mainly limited to the *intra*-EU level, while this chapter focuses on the grounds based on which EU data protection law applies "as a whole". This is what, in WP179, the A29WP calls the "external scope" of the EU data protection law, as "the extent to which EU data protection law is applicable to processing of personal data taking place wholly or partly outside the EU/EEA, but still having a relevant connection with the EU/EEA territory" (Ibid., 5.). From this broader perspective, applicable law and jurisdiction often go hand-in-hand.

Commission: "[t]he assertion of extraterritorial jurisdiction by a State is an attempt to regulate by means of national legislation, adjudication or enforcement the *conduct of persons, property or acts beyond its borders* which affect the interests of the State in the absence of such regulation under international law".[234] Along the same line, Senz and Charlesworth (2001) recall that "[t]he term 'extraterritoriality' is generally understood to refer to the exercise of jurisdiction by a state over *activities* occurring *outside* its borders". Precisely, "[t]he traditional international legal use of the term 'extraterritorial legislation' covers two different types of laws: legislation that regulates the *conduct of nationals abroad*, and laws that apply to *conduct by non-nationals outside* the territory of the legislating country".[235]

As suggested by Svantesson (2014), when determining whether a jurisdictional claim is extraterritorial or not (or at least, attempting to), the focus should not be on the location of the *activities* but on the location of natural or legal *person* that conduct those activities: "[p]ersons, whether legal or natural, are always located somewhere, while locating 'activities' may be more difficult".[236] A similar suggestion seems sensible in the data protection field if one considers that, in the context of cloud computing, pinpointing the location of the processing activities may result in an impossible task. Moreover, the focus on the location of the activities does not seem in line with the approach adopted under the Regulation, where, as it will be seen below, no attention is placed on the location of data processing activities. To stress this "shift" of focus, Svantesson proposed the following definition: "[a]n assertion of jurisdiction is extraterritorial as soon as it seeks to control or

[234] International Law Commission, *Report on the Work of Its Fifty- Eighth Session* (UN Doc. A/61/10, 2006), Annex E, paragraph 2 (italics mine), accessed January 2, 2019, https://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf. The adoption of this definition is suggested by Kuner (2015) "as a common-sense middle ground for understanding the term". Christopher Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law," *International Data Privacy Law* 5, no. 4 (2015): 238.

[235] Deborah Senz and Hilary Charlesworth, "Building Blocks: Australia's Response to Foreign Extraterritorial Legislation," *Melbourne Journal of International Law* 2, no. 1 (2001): 72 (italics mine).

[236] Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," 60–61. Svantesson noted that the definition of extraterritorial jurisdiction with a focus on the *activities* occurring outside national borders refers to the extraterritoriality "in scope", while the definition of extraterritorial jurisdiction with a focus on the *persons* that conduct those activities refers to the extraterritoriality "in effect".

otherwise directly affect the activities of an *object* (person, business, etc.) *outside* the territory of the state making the assertion".[237] This is the definition that will be adopted in the course of this chapter.

The grounds that under the 1995 Directive and the Regulation trigger the applicability of the EU data protection law are spelled out in Article 4 and Article 3 respectively.[238] The table below shows the differences in the wording of the two Articles:

Directive 95/46/EC Article 4 National law applicable	**Regulation (EU) 2016/679** Article 3 Territorial scope
1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;	1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller **or a processor** in the Union, **regardless of whether the processing takes place in the Union or not**.
(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;	
(c) the controller is not established on Community territory and, for purposes of processing personal data **makes use of equipment**, automated or otherwise, **situated on the territory of the said Member State**, unless such equipment is used only for purposes of transit through the territory of the Community.	2. This Regulation applies to the processing of personal data of **data subjects who are in the Union** by a controller or processor not established in the Union, where the processing activities are related to: (a) the **offering of goods or services**, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the **monitoring of their behaviour** as far as their behaviour takes place within the Union.
	3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Table 1 – Comparison DPD - GDPR

[237] Ibid., 60 (italics mine).

[238] The important difference between Article 4 of the 1995 Directive and Article 3 GDPR is that while "the main objective of Article 4 of the Directive was to define which Member State's national law is applicable", "Article 3 of the GDPR defines the territorial scope of a directly applicable text". European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 4.

Table 2 aims to summarize in a more schematic fashion the differences between the grounds on which the 1995 Directive and the Regulation become applicable:

Directive 95/46/EC Article 4 National law applicable	**Regulation (EU) 2016/679** Article 3 Territorial scope
NEXUS **1** (Art.4(1)(a)) Establishment of a controller in the Union + Processing carried out in the context of the activities of such establishment	NEXUS **1** (Art.3(1)) Establishment of a controller/processor in the Union[239] + Processing carried out in the context of the activities of such establishment
NEXUS **2** (Art.4(1)(c)) Controller not established in the Union + Equipment used for data processing situated in the Union[240]	NEXUS **2** (Art.3(2)) Controller/processor not established in the Union + Data subject in the EU + **a.** Processing activities related to the offering of goods or services to such data subject[241] (Art.3(2)(a)) or **b.** Processing activities related to the monitoring of their behaviour[242] (Art.3(2)(b))
NEXUS **3** (Art.4(1)(b)) Controller not established in the EU + Applicability of a Member State law by virtue of public international law	NEXUS **3** (Art.3(3)) Controller not established in the Union + Applicability of a Member State law by virtue of public international law

Table 2 – Schematic comparison DPD - GDPR

From the tables above, it is clear that neither under the 1995 Directive, nor under the Regulation, the physical location of personal data and of their processing is relevant to the applicability of EU data protection legislation (although under the 1995 Directive, the equipment criterion overlaps with the location of data processing).[243] In this respect, it should be recalled that under the original proposal of the 1995 Directive, the EU jurisdiction was determined by the location of the file.[244] However, this connecting factor was eventually – and wisely – dropped since, even back

[239] Regardless of whether the processing takes place in the Union or not.

[240] Unless such equipment is used only for purposes of transit through the territory of the Community.

[241] Irrespective of whether a payment of the data subject is required.

[242] As far as their behaviour takes place within the Union.

[243] W. Kuan Hon, Julia Hörnle, and Christopher Millard, "Which Law(s) Apply to Personal Data in Clouds?," in *Cloud Computing Law*, ed. Christopher Millard (Oxford: Oxford University Press, 2013), 221.

[244] Article 4, Commission of the European Communities, *Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data*, COM(90) 314 final-SYN 287 and 288. (Brussels, 1990), accessed November 24, 2019, http://aei.pitt.edu/3768/1/3768.pdf.: "1. Each Member State shall apply

in the nineties, it was clear that "processing operations may have more than one location and take place in several Member States, particularly in the case of data bases connected to networks, which are becoming increasingly frequent".[245] In the light of this, it is worth stressing from the very beginning of this analysis that the addition "regardless of whether the processing takes place in the Union or not" included in Article 3(1) of the Regulation (see table 1) has only made explicit an already well-established concept.

The broad scope of application of the EU data protection legislation is also clear at first sight. The purpose of such a broad application is "primarily to ensure that individuals are not deprived of the protection to which they are entitled under the Directive, and, at the same time, to prevent circumvention of the law".[246] This is also made explicit under the 1992 Amended Proposal for the Directive where the European Commission stated that Article 4 has identified the connecting factors that determine when data processing activities fall under the scope of the 1995 Directive in order to avoid "that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this".[247] The wording adopted in Article 3 GDPR seems to be grounded upon the same rationale since it retains and, to some extent, broadens the wide scope of application of the EU data protection law.

this Directive to: (a) all files located in Its territory; (b) the controller of a file resident in Its territory who uses from its territory a file located in a third country whose law does not provide an adequate level of protection, unless such use is only sporadic. 2. Each Member State shall apply Articles 5, 6, 8, 9, 10, 17, 18 and 21 of this Directive to a user consulting a file located in a third country from a terminal located in the territory of a Member State, unless such use is only sporadic. 3. Where a file is moved temporarily from one Member State to another, the latter shall place no obstacle in the way and shall not require the completion of any formalities over and above those applicable in the Member State in which the file is normally located".

[245] Commission of the European Communities, *Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (COM(92)422 final, 1992), 13, accessed April 12, 2018, http://aei.pitt.edu/10375/1/10375.pdf.

[246] Article 29 Data Protection Working Party, *WP179*, 9.

[247] Commission of the European Communities, *Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 13.

3.2.2. The Extra-territorial Reach of EU Law: Some Insights from other Areas of Law

Before moving to the details of the territorial applicability of the GDPR, it should be recalled that the need to determine whether EU law applies to situations with connections with different countries is not specific to the EU data protection framework. Establishing which law applies to situations with links with more than one country is a question of international law which arises in both the off-line and the online world.[248] Questions about the breadth and the scope of national laws across borders are "as old as legal thought itself"[249] but they have acquired a new dimension in the modern age of globalization where companies operate on a global scale and their strategies affect a variety of geographical markets.[250]

Some examples of the extra-territorial dimension of EU law are offered by competition law. In *Woodpulp*,[251] wood pulp producers and two of their trade associations, all having registered offices outside the European Union, brought an action before the European Court of Justice (ECJ) in order to annul a decision of the European Commission which found them in breach of Article 85(1) of the Treaty establishing the European Economic Community (EEC Treaty), now Article 101 of the Treaty on the Functioning of the European Union (TFEU). In the contested decision, the European Commission concluded that those companies had engaged in concerted practices to fix the price of wood pulp. In their submission, the applicants contested that the Commission had misinterpreted the territorial scope of Article 85 of the EEC Treaty since Community law could not regulate conducts adopted outside the European Union "merely by reason of the economic repercussions which that conduct produces within the Community".[252] The ECJ, however, held that the Commission had not

[248] Article 29 Data Protection Working Party, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites (WP56)*, 2002, 2, accessed January 2, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf.

[249] Luca Prete, "On Implementation and Effects: The Recent Case-Law on the Territorial (or Extraterritorial?) Application of EU Competition Rules," *Journal of European Competition Law & Practice* 9, no. 8 (October 1, 2018): 487.

[250] Ibid., 487–488.

[251] Judgement of 27 September 1988, *Ahlström Osakeyhtiö and Others v Commission*, Joined Cases 89/85, 104/85, 114/85, 116/85, 117/85 and 125/85 to 129/85, EU:C:1988:447.

[252] Ibid., paragraph 6.

made an incorrect interpretation of Article 85 of the EEC Treaty in applying competition rules to undertakings whose registered offices are established outside the European Union.[253] Indeed, the ECJ concluded that "where those producers concert on the prices to be charged to their customers in the Community and put that concertation into effect by selling at prices which are actually coordinated, they are taking part in concertation which has the object and effect of restricting competition within the common market within the meaning of Article 85 of the Treaty".[254] The decisive factor taken into account by the ECJ is hence the place where the agreement was implemented regardless of where the undertakings concerned were established.[255] Otherwise, as stressed by the Court, "if the applicability of prohibitions laid down under competition law were made to depend on the place where the agreement, decision or concerted practice was formed, the result would obviously be to give undertakings an easy means of evading those prohibitions".[256]

Along the same lines, as for the application of Article 101 TFEU, in *Béguelin*, the ECJ concluded that the "fact that one of the undertakings which are parties to the agreement is situate in a third country does not prevent application of that provision since the agreement is operative on the territory of the common market".[257] In *Intel*,[258] the ECJ confirmed the extraterritorial reach of competition rules in establishing that the European Commission has the jurisdiction under international law to punish conducts adopted outside the European Union if it is foreseeable that those conducts, "viewed as a whole", will have an immediate and substantial effect within the European Union. Moreover, the ECJ specified that "it is sufficient to take account of the *probable* effects of conduct on competition in order for the foreseeability criterion to be satisfied".[259] On this ground, Intel, a US-based company that develops and markets, among others, central processing units, was

[253] Ibid., paragraph 14.
[254] Ibid., paragraph 13.
[255] Niilo Jääskinen and Angela Ward, "The External Reach of EU Private Law in the Light of L'Oréal versus EBay and Google and Google Spain," in *Private Law in the External Relations of the EU*, ed. Marise Cremona and Hans-W Micklitz, 1st ed. (Oxford: Oxford University Press, 2016), 130–131.
[256] Ibid., paragraph 16.
[257] Judgment of 25 November 1971, *Béguelin Import v G.L. Import Export*, C-22/71, ECLI:EU:C:1971:113, paragraph 11.
[258] Judgment of 6 September 2017, *Intel Corp. v European Commission*, C-413/14 P, ECLI:EU:C:2017:632.
[259] Ibid., paragraph 51 (italics mine).

found to have committed an abuse of dominant position in breach of Article 102 TFEU for having implemented a strategy aimed at excluding its competitor Advanced Micro Devices Inc. from the market for processors, including in the EEA.[260]

Moving from competition law to the environmental legislation, in *Air Transport Association of America and Others*,[261] the ECJ was asked whether, by enacting a scheme for greenhouse gas emission allowance trading within the Community, the EU had breached principles of customary international law of territoriality and of States' sovereignty over their airspace in so far as the said scheme also applies to "parts of flights which take place *outside* the airspace of the Member States, including to flights by aircraft registered in third States".[262] In the case in question, the ECJ concluded that:

> In laying down a criterion for Directive 2008/101 to be applicable to operators of aircraft registered in a Member State or in a third State that is founded on the fact that those aircraft perform a flight which departs from or arrives at an aerodrome situated in the territory of one of the Member States, Directive 2008/101, inasmuch as it extends application of the scheme laid down by Directive 2003/87 to aviation, does not infringe the principle of territoriality or the sovereignty which the third States from or to which such flights are performed have over the airspace above their territory, since those aircraft are physically in the territory of one of the Member States of the European Union and are thus subject on that basis to the unlimited jurisdiction of the European Union.[263]

In other words, the ECJ acknowledged that European Union law must be interpreted and applied in the light of customary rules of international law of the sea and of the air and, in compliance with those rules, EU law cannot apply to international flights flying over the territory of the Member States of the European Union when those flights do not depart nor land from those territories. On the other hand, aircrafts situated in the aerodrome of a Member State are "subject to the unlimited jurisdiction

[260] For a detailed analysis of the case, see Prete, "On Implementation and Effects: The Recent Case-Law on the Territorial (or Extraterritorial?) Application of EU Competition Rules," 490–492; Eleanor M. Fox, "Extraterritorial Jurisdiction, Antitrust, and the EU Intel Case: Implementation, Qualified Effects, and the Third Kind Essays," *Fordham International Law Journal* 42, no. 3 (2019): 981–998. For an overview of the extraterritorial reach of competition law, see also Giorgio Monti, "The Global Reach of EU Competition Law," in *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, ed. Marise Cremona and Joanne Scott, 1st ed. (Oxford: Oxford University Press, 2019).

[261] Judgment of 21 December 2011, *Air Transport Association of America and Others*, C-366/10, ECLI:EU:C:2011:864.

[262] Ibid., paragraph 112 (italics mine).

[263] Ibid., paragraph 125.

of that Member State and the European Union".[264] Moreover, the ECJ also stressed that the fact that "certain matters contributing to the pollution of the air, sea or land territory of the Member States originate in an event which occurs partly outside that territory is not such as to call into question, ... , the full applicability of European Union law in that territory".[265]

In *L'Oréal v. eBay*,[266] the ECJ stretched the boundaries of the external reach of EU trademark law. L'Oréal claimed that several transactions on eBay's European website had infringed its trade mark rights since the items in question were either non intended for sale or they were meant to be sold in North America and not in the European Union. On the other hand, eBay submitted that the proprietor of a trade mark registered in the European Union cannot rely on the rights conferred by that trade mark – in particular, the right to prevent third parties from importing goods bearing that trade mark – since "the goods bearing it and offered for sale on an online marketplace are located in a third State and will not necessarily be forwarded to the territory covered by the trade mark in question".[267] This argument was, however, rejected by the ECJ since it was clear, in its view, that the sale of trade-marked products located in a third country were targeted at consumers in the European Union and hence in territories covered by the trade mark:

> If it were otherwise, operators which use electronic commerce by offering for sale, on an online market place targeted at consumers within the EU, trade-marked goods located in a third State, which it is possible to view on the screen and to order via that marketplace, would, so far as offers for sale of that type are concerned, have no obligation to comply with the EU intellectual property rules. Such a situation would have an impact on the effectiveness (*effet utile*) of those rules.[268]

In other words, the ECJ contended that the very effectiveness of trade mark rules would be undermined if they were not applicable to the Internet offer for sale of goods targeted at consumers within the European Union merely because the party offering those goods is established in a third State or because the goods subject of the offer are located in a third State. In the light of this, it is up

[264] Ibid., paragraph 124.
[265] Ibid., paragraph 129.
[266] Judgment of 12 July 2011, *L'Oréal and Others*, C-324/09, ECLI:EU:C:2011:474.
[267] Ibid., paragraph 61.
[268] Ibid., paragraph 62.

to the national courts to assess whether an offer for sale "displayed on an online marketplace accessible from the territory covered by the trade mark" is targeted at consumers in that territory.[269]

At the same time, in *L'Oréal v. eBay*, the ECJ clarified that "the mere fact that a website is accessible from the territory covered by the trade mark is not a sufficient basis for concluding that the offers for sale displayed there are targeted at consumers in that territory".[270] Indeed, if the EU rules on intellectual property were to be applicable to advertisements displayed on an online marketplace merely because that marketplace is technically accessible from the EU territory even if they are exclusively targeted to consumers in third States, EU rules would wrongly apply to those advertisements.[271]

The need to adapt existing rules to the modern digital economy has also emerged in the taxation field. Under the current framework, the right to tax in a country and the amount of the corporate income allocated to that country is largely dependent on having a physical presence in the country in question. These rules hence fail to catch the digital transformation on which modern economy is based where profits are increasingly dependent on a digital, rather than on a physical, presence and where users play an essential role in generating value. For example, users contribute to value creation by sharing their data and their preferences online which are consequentially monetized by digital companies by means of targeted advertising. However, the profits generated by users are not always taxed in the country where those users are located. As a result of this mismatch between the place where value is created and the place where profits are taxed, the profits gained by the company thanks to the users' contribution are not taken into account.[272]

---

[269] Ibid., paragraph 65.

[270] Ibid., paragraph 64.

[271] Ibid., paragraph 64. In reaching this conclusion, the ECJ applied by analogy the principle established in the field of consumer protection in Judgment of 7 December 2010, *Pammer and Hotel Alpenhof*, Joined Cases C-585/08 and C-144/09, ECLI:EU:C:2010:740 (3.4.3.). For a detailed analysis of the principles established in *L'Oréal v. eBay*, see Jääskinen and Ward, "The External Reach of EU Private Law in the Light of L'Oréal versus EBay and Google and Google Spain," 138–140.

[272] European Commission, *Communication from the Commission to the European Parliament and the Council. Time to Establish a Modern, Fair and Efficient Taxation Standard for the Digital Economy*, COM(2018) 146 final. (Brussels, 2018), accessed June 22, 2020, https://eur-lex.europa.eu/resource.html?uri=cellar:2bafa0d9-2dde-11e8-b5fe-01aa75ed71a1.0017.02/DOC_1&format=PDF; European Commission, "Fair Taxation of the Digital Economy," last

The European Commission has hence made two legislative proposals in order to better capture value creation in modern business models. The first proposal[273] aims to reform current corporate tax rules for digital activities in order to enable Member States to tax profits generated in their territory even if companies have no physical presence there while still interacting substantially with users by means of digital channels. This would ensure that companies making their business online would contribute to public finance even if they have no physical presence in the territory of the country in question. Under the proposed directive, entities, "irrespective of where they are resident for corporate tax purposes, whether in a Member State or in a third country",[274] are deemed to have a significant digital presence in a country, and hence a taxable nexus in that country, "if the revenues from providing digital services to users in a jurisdiction exceed EUR 7 000 000 in a tax period, if the number of users of a digital service in a Member State exceeds 100 000 in a tax period or if the number of business contracts for digital services exceeds 3 000".[275] The economically significant activities performed by the entity with a significant digital presence that shall be taken into account in order to determine the profits attributable to that presence in a Member State include, *inter alia*, "the collection, storage, processing, analysis, deployment and sale of user-level data" and "the collection, storage, processing and display of user-generated content".[276]

The second proposal[277] aims to establish an interim tax – meaning that it would apply until a more comprehensive framework is established – in order to cover some digital activities that escape the current tax system entirely in order to ensure that those activities start generating revenue in the European Union.[278] The taxable revenues for the purposes of the proposed Directive would be the

modified September 20, 2017, accessed June 22, 2020, https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en.

[273] European Commission, *Proposal for a Council Directive Laying down Rules Relating to the Corporate Taxation of a Significant Digital Presence* (Brussels: COM(2018) 147 final, 2018).

[274] Article 2, Ibid.

[275] Ibid., 8.

[276] Article 5(5), European Commission, *Proposal for a Council Directive Laying down Rules Relating to the Corporate Taxation of a Significant Digital Presence*.

[277] European Commission, *Proposal for a Council Directive on the Common System of a Digital Services Tax on Revenues Resulting from the Provision of Certain Digital Services* (Brussels: COM(2018) 148 final, 2018).

[278] European Commission, "Fair Taxation of the Digital Economy."

revenues created from the selling of advertisement space targeted at users, from digital intermediary activities which allow users to interact and which "facilitate the provision of underlying supplies of goods or services directly between users" and from the "transmission of data collected about users and generated from users' activities on digital interfaces".[279] The tax would hence apply to the activities where end-users play a major role in value creation and would, indeed, be collected in the Member State where users are located. These two proposals of the European Commission are another example of the attempt of the European Union to adapt the current framework, designed for " 'brick-and-mortar' businesses", to the "boom in the digital economy" where more and more companies generate value online and make their profit from consumers' data regardless of where they are established.[280]

The analysis conducted above has shown that the international effects of EU law are generally grounded upon States' concern to protect the rights and the interests of their citizens and industry in order to ensure the protective effects of those rules. Under various circumstances and in different areas of law, the European Court of Justice as well as other European institutions have tried to expand the scope of application of the EU law so as to protect EU citizens and businesses as broadly as possible even if this extends the reach of EU law to conducts that take place in third countries. Establishing the grounds and the criteria that should be decisive in determining which law should apply in situations involving cross-frontier elements often raises major challenges. This derives from the fact that, in order to determine the applicable law in situations which have some form of connections with different countries, a fair balance should be struck between the various national interests of the countries involved. Such challenges have been exacerbated by the increasingly interconnected and globalized world in which we live where a wide range of conducts taking place

[279] Article 3(1), European Commission, *Proposal for a Council Directive on the Common System of a Digital Services Tax on Revenues Resulting from the Provision of Certain Digital Services*.

[280] European Commission, "Questions and Answers on a Fair and Efficient Tax System in the EU for the Digital Single Market," accessed June 22, 2020, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_2141. For an overview of the unilateral measures that have been taken at the national level by EU Member States, see Stefanie Geringer, "National Digital Taxes – Lessons from Europe," *South African Journal of Accounting Research* (March 23, 2020): 1–19.

outside the EU are likely to have an impact within. In the light of this, as acknowledged back in 2002 by the A29WP, it could be argued that the fact that the EU data protection framework contains "an explicit provision on the applicable law indicating a criterion" – however complex the interpretation and the application of that criterion might be – "it is nevertheless an advantage for the benefit of individuals and business" that fall under the scope of the EU data protection rules.[281] In the absence of such provision, the ECJ would indeed be required to solve similar issues on a case-by-case basis drawing from other fields of law which involve "extra-EU factual" elements.[282]

3.3. Nexus 1: Untangling the Establishment Criterion

3.3.1. The Establishment Criterion from a Public International Law Perspective

Article 3(1) of the GDPR provides that "[t]his Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not". From a public international law perspective, the establishment criterion can be seen as an expression of the territoriality principle, under which a State has jurisdiction over acts committed within its territory.[283] In this case, the link between the EU territory and the Regulation is represented by the location of the establishment of a controller or a processor within the EU boundaries.[284]

As a general remark, since Article 3(1) GDPR essentially replicates the jurisdictional nexus first introduced under Article 4(1)(a) of the 1995 Directive, several considerations that have already been expressed with reference to the key terms of Article 4(1)(a) of the said Directive can be extended to Article 3(1) of the Regulation. The establishment criterion is composed of two complementary

[281] Article 29 Data Protection Working Party, *WP56*, 5.

[282] Jääskinen and Ward, "The External Reach of EU Private Law in the Light of L'Oréal versus EBay and Google and Google Spain," 145–146.

[283] Cedric Ryngaert, *Jurisdiction in International Law*, Second ed. (Oxford, United Kingdom; New York, NY: Oxford University Press, 2015), 49.

[284] This opinion is shared by several commentators. Among others, Lokke Moerel, "The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?," *International Data Privacy Law* 1, no. 1 (2011): 29; Liane Colonna, "Article 4 of the EU Data Protection Directive and the Irrelevance of the EU–US Safe Harbor Program?," *International Data Privacy Law* 4, no. 3 (2014): 208.

requirements. First, it is necessary to verify whether a controller, or a processor,[285] has an establishment in the European Union; second, whether the processing of personal data is carried out in the context of the activities of that establishment.[286]

3.3.2. The Concept of "Establishment"

A correct understanding of the concept of "establishment" seems to be of primary importance. First, it should be noted that Article 3(1) of the Regulation, like Article 4(1)(a) of the 1995 Directive, does not refer to *the* establishment of the controller (or of the processor) but, more generally, to *an* establishment. This indicates that the attention of the EU co-legislator is not, or at least not only, on the place of formal registration of a parent company, but also on any secondary establishments, such as subsidiaries, branches and agencies.[287] This is made explicit under Recital 19 of the 1995 Directive and Recital 22 of the GDPR which provide that the legal form, whether a branch or a subsidiary with a legal personality, is not the decisive factor in determining whether a given "arrangement" can qualify as an establishment. A data controller may thus be required to comply with the data protection laws (implementing the 1995 Directive, now the Regulation) of various Member States if it has establishments in those States.[288] This situation was particularly problematic under the 1995 Directive since the national laws implementing the 1995 Directive were, under certain aspects, substantially different.

---

[285] The analysis of the difficulties in applying the concepts of "controller" and "processor" is beyond the scope of this chapter. For some important clarifications, see Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor" (WP169)*, 2010, accessed January 2, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. See also, European Data Protection Supervisor, *Guidelines on the Concepts of Controller, Processor and Joint Controllership under Regulation (EU) 2018/1725*, 2019, accessed January 2, 2019, https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf. It is worth recalling that the classification of an actor as a controller or a processor does not depend on the corporate structure of a given company although it can have an influence in this finding. Christopher Kuner, *European Data Privacy Law and Online Business* (New York; Oxford: Oxford University Press, 2003), 106–107.

[286] Hon, Hörnle, and Millard, "Which Law(s) Apply to Personal Data in Clouds?," 222.

[287] Lokke Moerel, "Back to Basics: When Does EU Data Protection Law Apply?," *International Data Privacy Law* 1, no. 2 (2011): 94–95.

[288] Article 29 Data Protection Working Party, *WP179*, 12.

Recital 22 of the Regulation also indicates that "[e]stablishment implies the effective and real exercise of activity through stable arrangements".[289] Needless to say, the interpretation of these criteria may raise several challenges in the context of real-world situations. Some guidance on how to interpret the concept of establishment is offered in WP179 where the A29WP suggested that the notion of "establishment" should be guided by the jurisprudence of the European Court of Justice concerning the freedom of establishment under Article 50 of the TFEU. Indeed, when drafting the 1995 Directive and, in particular, Recital 19, it is plausible that the EU co-legislators have been inspired by the clarifications provided by the EU courts with reference to the freedom of establishment.[290] Some clarifications are, for example, offered in *Berkholz v Finanzamt Hamburg-Mitte-Altstadt*, where the ECJ has affirmed that a stable establishment "entails the permanent presence of both the *human* and *technical* resources necessary for the provision of those services".[291] Similarly, in *Lease Plan Luxembourg v Belgische Staat*, the ECJ concluded that "an undertaking established in one Member State which hires out or leases a number of vehicles to clients established in another Member State does not possess a fixed establishment in that other State merely by engaging in that hiring out or leasing".[292] Indeed, "neither the physical placing of vehicles at customers' disposal under leasing agreements nor the place at which they are used can be regarded as a clear, simple and practical criterion, ..., on which to base the existence of a fixed establishment".[293]

Specific insights about the concept of establishment within the context of the 1995 Directive are provided in *Weltimmo*,[294] which shows how the broad wording adopted under Recital 19 of the 1995 Directive has been used by the ECJ for justifying a flexible definition of the concept of

[289] Recital 19 Directive and Recital 22 GDPR.
[290] Article 29 Data Protection Working Party, *WP179*, 11.
[291] Judgment of 4 July 1985, *Berkholz v Finanzamt Hamburg-Mitte-Altstadt*, C-168/84, ECLI:EU:C:1985:299, p.2265 (italics mine).
[292] Judgment of 7 May 1998, *Lease Plan Luxembourg v Belgische Staat*, C-390/96, ECLI:EU:C:1998:206, paragraph. 29.
[293] Ibid., paragraph 28.
[294] Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639 (hereafter cited as *Weltimmo*).

establishment.[295] Firstly, the ECJ reiterated that a company, i.e., the data controller, may have an establishment that falls under the meaning of the 1995 Directive in a Member State other than the one where it is formally registered. Secondly, it added that both the degree of stability of the arrangements and the effective exercise of activities through those arrangements "must be interpreted in the light of the specific nature of the economic activities" conducted by the undertaking in question, especially when it comes to companies that offer services only over the Internet.[296] In particular, it held that

> ... in the light of the objective pursued by that directive, consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, ... the presence of only *one* representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question. In addition, in order to attain that objective, it should be considered that the concept of 'establishment', within the meaning of Directive 95/46, extends to any real and effective activity — even a minimal one — exercised through stable arrangements.[297]

This case-law was also recalled by the EDPB in its Guidelines on the territorial scope of the GDPR in which the EDPB has stressed that the Regulation, just like the 1995 Directive, has departed from a formalistic approach whereby a data controller (or a data processor) is established exclusively in the place where it is registered or where is has a branch or a subsidiary. At the same time, the EDPB noted that "[a]lthough the notion of establishment is broad, it is not without limits".[298] However, where exactly these limits should be drawn and what factors should be taken into account

[295] Paul de Hert and Michal Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context," *International Data Privacy Law* 6, no. 3 (July 13, 2016): 233.

[296] *Weltimmo*, paragraph 29.

[297] Ibid., paragraphs 30-31. In the case in question, the ECJ concluded that Weltimmo, a company registered in Slovakia, conducted a *real* and *effective* activity in Hungary that consisted in the running of a property dealing website concerning properties located in Hungary. In particular, the *stable* arrangement was identified by the ECJ in the presence in Hungary of a representative of Weltimmo that served as the point of contact of the company for data subjects and that represented the company in all the administrative and judicial proceedings. The company had also opened a bank account in Hungary and had a letter box for managing daily business affairs. In conclusion, according to the ECJ, these elements are "capable of establishing, in a situation such as that at issue in the main proceedings, the existence of an 'establishment' within the meaning of Article 4(1)(a) of Directive 95/46" (paragraph 33).

[298] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 7.

in practice when assessing whether a controller or a processor has an establishment in the European Union are not clearly identified in these Guidelines.

An important clarification was, however, given by the EDPB as to whether a processor in the EU may be considered to be an establishment in the EU of a non-EU data controller. According to the EDPB, a similar situation does not necessarily trigger the applicability of the GDPR: "the EDPB notably deems that a processor in the EU should not be considered to be an establishment of a data controller within the meaning of Article 3(1) merely by virtue of its status as processor on behalf of a controller".[299] Simply put, the non-EU data controller would not automatically be caught under the scope of the GDPR merely because it decides to avail itself of a data processor located in the EU. Indeed, unless other factors are in place, when a non-EU data controller makes use of the processing activities of an EU data processor, the data controller is not carrying out processing activities in the context of the establishment of the processor. Such processing activities are conducted in the controller's own activities while "the processor is merely providing a processing service".[300]

Overall, the flexible interpretation of establishment proposed by the ECJ is certainly motivated by a laudable purpose: ensuring an effective and complete protection of the right to privacy. However, flexible interpretations are often developed at the expense of clarity. Indeed, although, theoretically, all companies (should) know where they are established, and (should) hence know when their activities are subject to EU law,[301] determining whether an "arrangement" can be counted as an establishment for the purpose of Article 4(1)(a) of the 1995 Directive, and now of Article 3(1) of the Regulation, may raise several practical challenges when the boundaries of the notion of establishment are so loose. Whether a data centre falls under the concept of "establishment" is, for example, unclear. Indeed, unlike a server that "is simply a technical facility or instrument for the processing of information",[302] a data centre "comprises a building, normally with employees to maintain the

[299] Ibid., 10.
[300] Ibid., 12.
[301] de Hert and Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context," 243.
[302] Article 29 Data Protection Working Party, *WP179*, 12.

servers, power, cooling, physical security, and so on".[303] Lack of clarity in the definition of this concept has also led to an inconsistent implementation of the establishment criterion across the European Union, where the interpretation developed in some countries is more expansive than the one adopted in others.[304] In the light of these uncertainties, the Regulation, although directly applicable, may also fail in achieving harmonization since it perpetuates the concept of establishment without additional clarifications, thus providing national data protection authorities with leeway for different interpretations.[305]

3.3.3. The Concept of "in the Context of the Activities of an Establishment"

Just like the notion of "establishment", the words "in the context of the activities of an establishment" that have been transposed from the 1995 Directive to the Regulation need some clarification. Once again, some guidance is offered by the A29WP. In WP179, in particular, the A29WP identified three elements that should be taken into account when determining whether the processing activities in question fall under the territorial scope of the EU data protection legislation. Firstly, it is crucial to determine "[t]he degree of involvement of the establishment(s) in the activities in the context of which personal data are processed". The degree of involvement should be measured on the basis of the "who is doing what" check: "which activities are being carried out by which establishment, so as to be able to determine whether the establishment is relevant in order to trigger the application of national data protection law".[306] Secondly, the nature of the activities of the establishment needs to be taken into account: the question whether an activity also involves personal data and whether the data processing activities are performed in the context of the activities of an establishment in the EU largely depends on the nature of the activities of the EU establishment.

[303] Hon, Hörnle, and Millard, "Which Law(s) Apply to Personal Data in Clouds?," 232.
[304] Kuner, *European Data Privacy Law and Online Business*, 66.
[305] Hon, Hörnle, and Millard, "Which Law(s) Apply to Personal Data in Clouds?," 245.
[306] Article 29 Data Protection Working Party, *WP179*, 14.

Thirdly, the objective of the 1995 Directive of ensuring effective data protection "in a simple, workable and predictable way" should also guide the analysis.[307]

Further clarifications have been provided by the A29WP with specific reference to search engines: the requirement that the processing operations are carried out "in the context of the activities of an establishment of the controller" means that the establishment should play a relevant role in those particular processing activities. This is the case when the establishment located in the European Union is responsible for relations with search engine users, when it complies with law enforcement requests with regard to users, and when the office that a search engine provider has established in a Member State is in charge of selling advertisements to the inhabitants of that State.[308] In other words, as it was further stressed by the EDPB in its Guidelines on the territorial scope of the Regulation, on the one hand, in order to ensure effective and complete protection to data subjects, the concept of "in the context of the activities of an establishment" should not be interpreted (too) restrictively. On the other hand, the same concept should not be interpreted too broadly "to conclude that the existence of any presence in the EU with even the remotest links to the data processing activities of a non-EU entity will be sufficient to bring this processing within the scope of EU data protection law".[309]

Some important clarifications on how the concept in question should be interpreted were given by the ECJ in *Google Spain*.[310] The question raised in *Google Spain* was whether, under the 1995 Directive, Google could be requested to remove information about a person from the list of results displayed after a search made on the basis of the person's name. The central question was whether the Spanish data protection law, implementing the 1995 Directive, was applicable to Google considering that the operator of the search engine, Google Inc., has its seat in the United States and that its Spanish subsidiary, Google Spain, is a commercial agent for the Google group, selling

[307] Ibid.

[308] Article 29 Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines (WP148)*, 2008, 10, accessed January 2, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.

[309] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 7.

[310] Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317 (hereafter cited as *Google Spain*).

advertising space mainly to undertakings based in Spain. With reference to the territorial scope of the 1995 Directive, the ECJ clarified that "Article 4(1)(a) of Directive 95/46 does not require the processing of personal data in question to be carried out 'by' the establishment concerned itself, but only that it be carried out 'in the context of the activities' of the establishment".[311] From this followed that, given that "the operation of loading personal data on an internet page must be considered to be" processing of those data[312] and that the operator of a search engine shall be regarded as controller in respect of that processing,[313] "the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State" – in this case Google Inc. – "but has an establishment in a Member State" – in this case Google Spain – "is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable".[314]

Indeed, "the activities of the operator of the search engine [Google Inc.] and those of its establishment situated in the Member State concerned [Google Spain] are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed".[315] In other words, on the one hand, Google Inc. could not perform its activities as an operator of a search engine without the profits gained through the activities relating to the selling of advertising space carried out by Google Spain; on the other hand, the search engine itself is, in turn, the means that allows Google Spain to perform its activities since the display of personal data

[311] *Google Spain*, paragraph 52.

[312] Ibid., paragraph 26. The ECJ clarified that "in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data" (paragraph 28).

[313] Ibid., paragraphs 32-33.

[314] Ibid., paragraph 55.

[315] Ibid., paragraph 56.

on a search results page "is accompanied, on the same page, by the display of advertising linked to the search terms".[316] It is also worth stressing that the location of data processing operations had no relevance in this reasoning. As suggested by Advocate General Jääskinen, "processing of personal data takes place within the context of a controller's establishment if that establishment acts as the bridge for the referencing service to the advertising market of that Member State, even if the technical data processing operations are situated in other Member States or third countries".[317]

Once again, the extensive interpretation of the notion of "in the context of the activities of an establishment" was justified by the necessity to meet the objective of the 1995 Directive, i.e., ensuring "*effective* and *complete* protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data".[318] As de Hert and Czerniawski (2016) have noted, in *Weltimmo* and *Google Spain*, the ECJ has given a *teleological* interpretation of the relevant legal provisions by interpreting and understanding the words used by the EU co-legislators in the light not only of the underpinning objectives of the EU data protection legislation (and hence of the protection of the right to privacy), but also of their broader legal framework (and hence of the effective protection of fundamental rights that permeates the EU legal system).[319]

The cases analysed above show that the connection with the EU territory as a trigger for the EU data protection legislation – represented by the presence of an establishment within the EU – was loosened by the ECJ in order to meet the objective of the 1995 Directive. A case-by-case analysis is hence necessary in order to verify whether there is an inextricable link between the activities of an EU establishment and the data processing activities of a non-EU controller or processor. If such a link is identified, "EU law will apply to that processing by the non-EU entity, whether or not the EU

[316] Ibid., paragraph 57.
[317] Opinion of Advocate General Jääskinen delivered on 25 June 2013, *Google Spain and Google*, C-131/12, ECLI:EU:C:2013:424, paragraph 67.
[318] *Google Spain*, paragraph 53 (italics mine).
[319] de Hert and Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context," 234–235.

establishment plays a role in that processing of data".[320] Again, however, extensive interpretations can raise uncertainties. Indeed, the "wide view of 'context' arguably risks rendering 'context' as a connecting factor meaningless"[321] thus leading to legal uncertainties as to the applicability of the EU law. This analysis shows that all the uncertainties that have been highlighted under Article 4(1)(a) of the 1995 Directive will be inherited by Article 3(1) of the Regulation which, as tables 1 and 2 show, replicates the wording of the DPD without clarifying its key notions nor has the EDPB added elements of clarification. Moreover, since Article 3(1) GDPR extends the applicability of the establishment criterion to processors (3.3.4.), the current problems of interpretation of the notions of "establishment" and "in the context of the activities of an establishment" are likely to be extended to processors.[322]

3.3.4. The Application of the Establishment Criterion to Data Processors

It is relevant that the Regulation, as opposed to the 1995 Directive, does not refer exclusively to the establishment of a controller, but also to the establishment of a processor. By bringing processors under the direct scope of the GDPR, the EU co-legislators aim to "prevent situations where a legal gap would allow the EU being used as a data haven, for instance when a processing activity entails inadmissible ethical issues".[323] By virtue of this addition, processors become *directly* subject to the EU legislation. Cloud providers, for example, may become directly subject to the Regulation, since most of the time they are not controllers but processors on behalf of their business customers.[324] This implies that EU processors fall directly within the scope of the Regulation even when the

[320] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 8.

[321] Hon, Hörnle, and Millard, "Which Law(s) Apply to Personal Data in Clouds?," 225.

[322] Ibid., 244.

[323] Article 29 Data Protection Working Party, *WP179*, 31–32. This concept was also reiterated by the EDPB in its Guidelines on the territorial scope of the GDPR. Indeed, according to the EDPB, certain legal obligations will need to be respected by EU data processors regardless of the location of the data controller on behalf of which they are carrying out their processing activities. European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 13. See also, Lokke Moerel, "GDPR Conundrums: The GDPR Applicability Regime — Part 2: Processors," February 6, 2018, accessed April 10, 2018, https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-2-processors/.

[324] Hon, Hörnle, and Millard, "Which Law(s) Apply to Personal Data in Clouds?," 231 and 244.

controller on behalf of which they process data is not subject to the Regulation[325] (this is scenario 1 – see table 3 below). However, as clarified by the EDPB in its Guidelines 3/2018, only *some* GDPR provisions are directly applicable to the EU processors (the "GDPR processor obligations"):

- the duty to enter into an agreement with the data controller with the exception of the obligation to assist the controller in complying with its own obligations and the obligation to process data only following the instructions of the data controller;
- the obligation to maintain a record of all categories of processing activities carried out on behalf of the data controller pursuant to Article 30(2) GDPR;
- the obligation to cooperate with the Supervisory Authority;
- the obligation to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk pursuant to Article 32 GDPR and to notify the data controller in the event of a data breach;
- the obligation to appoint a data protection officer (DPO), where applicable, and
- the obligation to comply with the rules on international data transfer.[326]

Moreover, the EDPB recalled that processors are required to ensure that their processing activities remain compliant with the EU data protection framework. This entails that, pursuant to Article 28(3) GDPR, EU processors are required to inform the non-EU controller if its instructions infringe the GDPR or national data protection provisions.[327]

The implementation of these obligations may, however, raise several practical challenges. For example, it is hard to imagine how data processors can maintain a record of the processing activities it carries out on behalf of a non-EEA data controller when the data controller itself is not subject to

[325] This is for example the case of a processor based in Spain who enters into a contract with a retail company based in Mexico for the processing of its clients' data. The Mexican company is exclusively targeting people outside the EU. According to the EDPB, in a similar scenario, the Mexican company is not subject to the GDPR regardless of the fact that it has decided to make use of the processing service of a data processor based in the EU. At the same time, the data processor based in Spain will be subject to the processor obligations imposed by the GDPR. European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 12.

[326] Ibid., 12–13.

[327] Ibid., 13.

the GDPR and is hence not bound to keep track of its own processing activities. In this respect, it should also be considered that the ultimate aim of mapping the processing activities is to ensure an efficient exercise of data subjects' rights. However, data subjects would not be entitled to exercise the data protection rights set out under the Regulation since, in the present scenario, the data controller against which such rights could be exercised is not subject to the GDPR. The obligation to immediately inform the controller if it thinks that an instruction infringes the Regulation seems also unreasonable: the data controller is not subject to the GDPR and it is hence expected that its obligations may not be compliant with the GDPR requirements. Likewise, it is hard to imagine how EU data processors can impose on non-EU data controller to enter into an agreement under Article 28 in a context where the data controller is not subject to the GDPR. The non-EU data controller could, indeed, reasonably refuse to enter into this GDPR-specific agreement with the consequence that the data processor may be held accountable for having failed to "force" the data controller to enter into such agreement.[328] As suggested by the Centre for Information Policy Leadership (CILP) in its comments on the draft EDPB's Guidelines on the territorial scope, "the EU processor should only have to meet the GDPR requirements to the extent they are in its exclusive sphere and control".[329] The invitation by the CILP to frame the GDPR processor obligations more pragmatically when data processors act on behalf of non-EU data controllers which are not subject to the GDPR was, however, not taken into consideration by the EDPB in its final Guidelines on the territorial scope.

[328] Centre for Information Policy Leadership, *Comments on the European Data Protection Board's "Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)" Adopted on 16 November 2018*, 2019, 9–10, accessed May 3, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_edpbs_territorial_scope_guidelines.pdf.

[329] Ibid., 10. On the same point, see also American Chamber of Commerce to the European Union, *Our Position - Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, 2019, 3, accessed May 2, 2019, http://www.amchameu.eu/system/files/position_papers/amchameu_edpb_guidelines_on_territorial_scope.pdf; Bitkom, *Views on EDPB Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, 2019, 9, accessed May 2, 2019, https://www.bitkom.org/sites/default/files/2019-01/20190118_Bitkom%20Position%20Paper%20EDPB%20Guidelines%20on%20the%20Territorial%20Scope%20%283%29.pdf; Business Software Alliance, *The Software Alliance's Response to the EDPB Public Consultation on the Proposed Guidelines on the Territorial Scope of the GDPR* (Brussels, 2019), 2, accessed May 2, 2019, https://www.bsa.org/sites/default/files/2019-02/01182019BSAResponseEDPBPublicConsultationonProposedGuidelinesonTerritorialScopeofGDPR.pdf.

Lets' now consider the scenario (scenario 2) where the non-EEA controller that outsources some processing activities to an EU processor is subject to EU law (i.e., the controller has no establishment in the European Union *but* targets or monitors data subjects in the EU thus triggering Article 3(2) GDPR). In this case, Article 28 GDPR will apply by requiring the non-EEA controller to impose on the EU processor a DP Agreement detailing the obligations with which the processor will need to comply. As a result, the EU processor will be subject both to the GDPR obligations that are directly applicable to processors and to the obligations under the DP Agreement stipulated with the controller.[330] To sum up:

Scenario 1	Non-EEA data controller not established in the EEA that does *not* target/monitor people in the EEA	+	EEA data processor	➡	The EU processor has to comply with the GDPR obligations that are directly applicable to processors
Scenario 2	Non-EEA data controller not established in the EEA that targets/monitors people in the EEA	+	EEA data processor	➡	The EU processor has to comply with: (1) the GDPR obligations that are directly applicable to processors *and* (2) with the obligations under the DP Agreement stipulated with the controller

Table 3 – GDPR processor obligations

3.4. Nexus 2: Untangling the Targeting and Monitoring Criteria

3.4.1. The Targeting and Monitoring Criteria from a Public International Law Perspective

Under Article 3(2)(a) GDPR, "[t]his Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; the monitoring of their behaviour as far as their behaviour takes place within the Union". From a public international law perspective, both the targeting and the monitoring criteria seem to fall under the passive personality principle, or at least, a revised form of it. Indeed, while under the (traditional) passive personality principle, jurisdiction is triggered by the nationality of the victim,[331] the targeting and the monitoring

[330] For an overview of all the possible scenarios, see Moerel, "GDPR Conundrums: The GDPR Applicability Regime — Part 2: Processors."

[331] Ryngaert, *Jurisdiction in International Law*, 110.

criteria place the focus not on the citizenship of data subjects, not even on their residency, but on their presence in the European Union. These jurisdictional grounds seem also to fall under the so-called "effects doctrine", or "effects principle", "under which a state has jurisdiction over foreign conduct which has certain effects within that state".[332] Indeed, the foreign conduct that by virtue of these grounds is attracted under the EU legislation has effects within the EU jurisdiction.[333]

3.4.2. The Replacement of the Equipment Criterion

Before moving to the analysis of Nexus 2 of the Regulation, it is useful to recall the basic characteristics of the nexus that the targeting and the monitoring criteria have replaced, i.e., the equipment criterion prescribed under Article 4(1)(c) of the 1995 Directive. From a public international law perspective, the equipment criterion can be traced back to the objective territorial principle (under which a "State can exercise jurisdiction if the act has been initiated abroad, but completed in its territory"[334] or when "a constitutive element of the conduct sought to be regulated occurred in the territory of the State"),[335] since it is partly based on the commission of an act within the European Union (through the equipment).[336] At the same time, the equipment criterion can also be seen as an expression of the effects doctrine since the focus is not on the use of the equipment located in the European Union *per se*, but rather on the fact that the foreign conduct is felt in the EU jurisdiction.[337] As noted by Kuner (2010): "Article 4(1)(c) is focused not on the use of equipment per se, but on preventing data controllers from evading EU rules by relocating outside the EU. Thus, Article 4(1)(c) also focuses on the effect produced in the EU by data processing outside the EU, and

[332] David J. Gerber, "Beyond Balancing: International Law Restraints on the Reach of National Laws," *Yale Journal of International Law* 10 (1984): 190.

[333] Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," 85. It should be noted that Svantesson reached this conclusion when the targeting and the monitoring criteria were still revolving around the data subject's *residency*. However, although the reference to the residency has been dropped in the final text, the argument remains sound.

[334] Ryngaert, *Jurisdiction in International Law*, 78–79.

[335] International Law Commission, *Report on the Work of Its Fifty- Eighth Session*, Annex E, paragraph 11.

[336] Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part I)," *International Journal of Law and Information Technology* 18 (2010): 188. See also, Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," 84.

[337] Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," 85.

the protection of EU citizens, meaning that it can also be viewed as an application of the effects doctrine".[338]

The equipment criterion was designed to expand the EU jurisdiction to data controllers with no physical presence in the EU that could be considered as an establishment under Article 4(1)(a) of the 1995 Directive or where the processing of personal data was not carried out in the context of the activities of such an establishment but where the processing of personal data had a clear connection with the EU territory represented by the use of equipment located in a Member State.[339] The goal of the provision was to avoid the circumvention of the EU data protection law that could result from the relocation of an establishment outside the European Union. This aim is made explicit in Recital 20 of the 1995 Directive: "the fact that the processing of data is carried out by a person established in a third country" – which would exclude the application of Article 4(1)(a) DPD – "must not stand in the way of the protection of individuals provided for in this Directive". Rather, "in these cases, the processing should be governed by the law of the Member State in which the means used are located",[340] and hence in accordance with Article 4(1)(c) of the 1995 Directive.

The "equipment" that triggered the EU jurisdiction under Article 4(1)(c) has been defined by the A29WP as "a set of tools or devices assembled for a specific purpose", such as personal computers, terminals or servers that can be used for any sort of processing. At the same time, equipment that is exclusively used for transit reasons, such as cables, fall outside the scope of Article 4(1)(c) of the 1995 Directive.[341] This seemingly straightforward definition has been (over)stretched thus leading to a(n) (over)broad understanding of the notion of equipment, as well as of the determination of when a controller "makes use" of such an equipment. Indeed, on the one hand, the A29WP has made clear that the word "equipment" should be interpreted as "means" so leading to "a broad interpretation of the criterion, which thus includes human and/or technical intermediaries, such

[338] Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part I)," 190.
[339] Article 29 Data Protection Working Party, *WP179*, 18.
[340] Recital 20 1995 Directive.
[341] Article 29 Data Protection Working Party, *WP56*, 9.

as in surveys or inquiries".[342] On the other hand, "making use of equipment" implies neither full control over equipment nor the ownership of the equipment. Rather, it presupposes "some kind of activity undertaken by the controller and the intention of the controller to process personal data".[343]

As a practical example of this broad interpretation, it is worth recalling that the A29WP, in its Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56), concluded that also users' personal computers located in the EU can be considered as equipment of which non-EU data controllers can "make use" by installing cookies. Cookies are text files installed on the hard disk of users' personal computers and that collect several information about the users such as the pages they have accessed, their identification number, and the advertisements they have clicked on. Cookies hence allow the controller to gather the information collected throughout the different sessions thus leading to a "quite detailed user profiles".[344] In this context, according to A29WP, the user's personal computer can be viewed as "equipment" within the scope of the 1995 Directive: "[i]t is located on the territory of a Member State [and] [t]he controller decided to use this equipment for the purpose of processing personal data".[345] The same reasoning was extended to the use of JavaScript, banners and other monitoring software applications.[346]

Such interpretations, however, seem to be at odds with the "cautious" approach that the A29WP itself, in the same working document, suggested that should be adopted in applying the equipment criterion to concrete cases: the objective of this criterion "is to ensure that individuals enjoy the protection of national data protection laws and the supervision of data processing by national data protection authorities in those cases where it is *necessary*, where it *makes sense* and where there is a *reasonable* degree of *enforceability* having regard to the cross-frontier situation

[342] Article 29 Data Protection Working Party, *WP179*, 20.
[343] Article 29 Data Protection Working Party, *WP56*, 9.
[344] Ibid., 10.
[345] Ibid., 11.
[346] Ibid., 11–12.

involved".[347] To the contrary, the interpretation suggested by the A29WP may lead to the applicability of the 1995 Directive to *all* online services that require EU users to login and that handle the login by installing cookies on the user's personal computer. Equally, all services, such as many websites, that do not require a login but still use cookies may be caught under the scope of the 1995 Directive as they come into contact with users in the EU,[348] thus leading to a "possible universal application of EU law".[349]

In WP179, the A29WP acknowledged that a broad understanding of the key terms of the equipment criterion could lead to some unsatisfactory consequences, especially when "the result is that European data protection law is applicable in cases where there is a limited connection with the EU (e.g. a controller established outside the EU, processing data of non-EU residents, only using equipment in the EU)".[350] This (overly) broad interpretation of the equipment criterion, and the resulting (overly) broad applicability of the DPD seem also to be inconsistent with the interpretation that the ECJ has given to the Chapter IV of the 1995 Directive ("Transfer of personal data to third countries") when, in *Lindqvist*, it concluded that the regime of the transfer of data should *not* become a "regime of *general* application, as regards operations on the internet"[351] (4.4.). Although this finding was made with reference to the data transfer rules, it should also guide the broader application of the EU data protection rules.[352]

3.4.3. The Application of the Targeting Criterion

Nexus 2 applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the European Union, where the processing activities are related to the offering of goods or services to those data subjects. It should be noted that the EU

[347] Ibid., 9 (italics mine).
[348] Hon, Hörnle, and Millard, "Which Law(s) Apply to Personal Data in Clouds?," 230–231.
[349] Article 29 Data Protection Working Party, *WP56*, 31.
[350] Ibid., 21.
[351] Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraph 69 (italics mine).
[352] Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 2nd ed. (New York; Oxford: Oxford University Press, 2007), 124.

jurisdiction does not seem to be triggered when non-EU companies offer goods or services to EU businesses (business-to-business relationships) since the Regulation only refers to the offering of goods and services to "data subjects", and hence natural persons (business-to-consumer relationships). The concept of service is explained under Article 57 TFEU. Services "shall be considered to be 'services' within the meaning of the Treaties where they are *normally* provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement for goods, capital and persons. Services' shall in particular include: (a) activities of an industrial character; (b) activities of a commercial character; (c) activities of craftsmen; (d) activities of the professions".[353] The concept of goods is instead governed by Article 28(2) TFEU. No definition of this concept is provided under the TFEU, but it can be identified in any set of products that can be shipped across boundaries and that have an intrinsic commercial value.[354]

The aim of this nexus is to avoid the circumvention of the law by controllers (and processors) through the relocation of their establishment(s) outside the European Union. This ultimate aim is made explicit under Recital 23 of the Regulation:

> In order to ensure that natural persons are *not deprived* of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by *a controller or a processor not established in the Union* should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.[355]

Article 3(2) GDPR hence extends the EU jurisdiction to controllers and processors established outside the EU and with no establishment therein that could make EU law applicable under Article 3(1) GDPR. Nexus 2 has been designed as a residual ground that comes into play only where the first nexus does not apply: when a controller has an establishment in Member State A, and offers goods

[353] Article 57 TFEU (italics mine).

[354] Judgement of 9 July 1992, *Commission v Belgium*, C-2/90, ECLI:EU:C:1992:310, paragraphs 23-26. On the definition of goods and services, see also Practice, *Risk-Aware Deployment and Intermediate Report on Status of Legislative Developments in Data Protection*, 2015, 13, accessed April 10, 2018, https://practice-project.eu/downloads/publications/Deliverables-Y2/D31.2-Risk-aware-deployment-PU-M24.pdf.

[355] Recital 23 GDPR (italics mine).

or services to Member States B and C, the processing activities related to the offering of goods and services to data subjects in B and C will also be dragged under the law of Member State A.[356]

Under the initial proposal of the European Commission, the EU jurisdiction was extended in in such a way that it would have applied to the processing of personal data of all data subjects *residing* in the European Union. The EU legislation was hence designed to follow EU residents in any part of the world so that, for example, a EU resident doing shopping in New York would have been entitled to demand the standards of protection laid out under the Regulation with reference to the data collected by the shops despite the strong link between that EU data subjects and US law, represented by the US soil.[357] In the final text, however, the reference to data subjects *residing* in the EU was replaced by a more general reference to data subjects *in* the EU.[358] This allows a generalized application of EU data protection legislation to all people physically present in the European Union, irrespective of their residency or nationality.[359] The applicability of EU data protection law to people *in* the EU seems to be more consistent with the EU conception of privacy as a fundamental right that should be enjoyed by everyone regardless of residency and nationality. This is also confirmed by Recital 14 GDPR which clarifies that the "the protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data".[360] Unlike the nationality and the legal status of the data subject, the location of the data subject is a determining factor under Article 3(2) GDPR. In this regard, the EDPB has clarified

[356] Lokke Moerel, "GDPR Conundrums: The GDPR Applicability Regime — Part 1: Controllers," January 29, 2018, accessed April 13, 2018, https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/.

[357] Dan Jerker B. Svantesson, "Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation," *International Data Privacy Law* 5, no. 4 (2015): 230.

[358] The amendments proposed by different committees of the EU Parliaments are available here: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2013-0402&language=EN.

[359] Colonna, "Article 4 of the EU Data Protection Directive and the Irrelevance of the EU–US Safe Harbor Program?," 214. On the other hand, the geographical location of data subjects is not relevant under Article 3(1) GDPR. As clarified by the EDPB in its Guidelines 3/2018, the "text of Article 3(1) does not restrict the application of the GDPR to the processing of personal data of individuals who are in the Union. The EDPB therefore considers that any personal data processing in the context of the activities of an establishment of a controller or processor in the Union would fall under the scope of the GDPR, regardless of the location or the nationality of the data subject whose personal data are being processed". European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 10.

[360] Recital 14 GDPR.

that the "requirement that the data subject be located in the Union must be assessed at the moment when the relevant trigger activity takes place, i.e. at the moment of offering of goods or services or the moment when the behaviour is being monitored, regardless of the duration of the offer made or monitoring undertaken".[361]

Two more changes can be identified from the original proposal of the European Commission. The first change is represented by the explicit reference to the fact that EU data protection law applies "irrespective of whether a payment of the data subject is required". This addition was proposed by the Committee on Civil Liberties, Justice and Home Affairs of the EU Parliament (LIBE Committee) in order to cover "all processing activities related to services, regardless of the fact whether or not these services are free of charge. This addition ensures the applicability of the Regulation to so-called 'free services'".[362] In other words, whether an activity conducted by a controller or a processor can be considered as an offer of goods or services under the scope the Regulation is not dependent upon the fact that payment is required in exchange of that offer.[363]

With reference to the second change, the European Parliament suggested to extend the scope of the Regulation to the processing activities conducted not only by a controller but also by a *processor* not established in the European Union.[364] Once again, this addition was designed to make the Regulation directly applicable to any entity that processes data of data subjects in the EU.[365] The applicability of Article 3(2) to non-EU data processors has raised several interpretative questions since data processors are generally processing data following the instructions of the data controller. This entails that who is actually targeting is not the data processor but the data controller. This was

[361] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 15.

[362] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 63.

[363] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 16.

[364] European Commission - MEMO, "LIBE Committee Vote Backs New EU Data Protection Rules," last modified October 22, 2013, accessed March 24, 2018, http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

[365] Colonna, "Article 4 of the EU Data Protection Directive and the Irrelevance of the EU–US Safe Harbor Program?," 214.

confirmed by the EDPB in its Guidelines on the territorial scope of the GDPR in which it stated that the decision to target individuals in a specific geographical area can only be made by an entity acting as a controller. In this context, "[w]hen it comes to a data processor not established in the Union, in order to determine whether its processing may be subject to the GDPR as per Article 3(2), it is necessary to look at whether the processing activities by the processor 'are related' to the targeting activities of the controller".[366]

In other words, in order to establish whether a non-EU data processor is directly subject to the GDPR, it is necessary to examine whether a connection can be traced between the targeting activities carried out by the data controller and the processing activities conducted by the data processor.[367] Despite this clarification, the added value of the *direct* applicability of the Regulation to non-EU data processors that target data subjects in the EU on behalf of a non-EU data controller seems to be fairly limited. Indeed, in a similar scenario, the non-EU data controller would be caught under the territorial scope of the GDPR and will hence be required to implement its provisions, including those under Article 28 GDPR. The contractual arrangements stipulated between the non-EU data controller and the non-EU data processor by virtue of Article 28 GDPR would hence make the non-EU data processors indirectly subject to the GDPR. Simply put, the (*indirect*) applicability of the GDPR to non-EU data processors could be assured even in the absence of a specific provision which makes the Regulation *directly* applicable to non-EU processors. What is worse, the interpretation given by the EDPB may entail that, in order for a non-EU data processor to know whether it is directly subject or not to the GDPR pursuant to Article 3(2) GDPR, the non-EU processors would be required "to verify for each and every one of their corporate customers (wherever they are located in the world),

[366] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 21.

[367] Ibid. The EDPB offered the following example: "A Brazilian company sells food ingredients and local recipes online, making this offer of good available to persons in the Union, by advertising these products and offering the delivery in the France, Spain and Portugal. In this context, the company instructs a data processor also established in Brazil to develop special offers to customers in France, Spain and Portugal on the basis of their previous orders and to carry out the related data processing. Processing activities by the processor, under the instruction of the data controller, are related to the offer of good to data subject in the Union. Furthermore, by developing these customized offers, the data processor directly monitors data subjects in the EU. Processing by the processor are therefore subject to the GDPR, as per Article 3(2)".

whether these customers target individuals in the EU for services or goods or monitor their behaviour".[368] This interpretation would clearly burden non-EU processors with an impossible task, considering that the activities conducted by their customers may also change over time.[369]

After having examined the various elements on which the jurisdictional ground under Article 3(2) GDPR is based (i.e., the concept of "goods" and the concept of "services", the relevance of the location of the data subjects, the applicability of the GDPR to the so-called "free services", and the applicability of Article 3(2) to the processing activities of both data controllers and processors), it is time to analyse the concept of "offering of goods or services". Indeed, as clarified by the EDPB, the fact that the processing activities concern individuals in the EU is not sufficient to trigger the applicability of the GDPR: the element of targeting must be present in addition.[370] Other crucial challenges may arise when interpreting the concept of "offering of goods or services". In the light of this wording, two situations may arise:

1) a company actively endeavours to win customers in the EU market but fails to do so;
2) a company wins customers in the EU market even though it does not actively endeavour to do so.[371]

With reference to the first situation, it is clear from the wording chosen by the EU co-legislators that the Regulation would apply. Article 3(2)(a), in fact, does not refer to the "supplying" of goods or services but merely to the "offering" of goods or services. The applicability of the GDPR to the second situation is instead not so straightforward at first sight. The online market is, indeed, populated by many companies that act at a global level without specifically targeting individuals in the EU. In these situations courts may face an all-or-nothing choice of concluding either that such companies target "every country in the world", including the EU, or "no countries at all".[372] The

[368] Moerel, "GDPR Conundrums: The GDPR Applicability Regime — Part 2: Processors."
[369] Ibid.
[370] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 15.
[371] Svantesson, "Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation," 232.
[372] Ibid.

complexity of the problem is clearly pictured by de Hert and Czerniawski (2016) when they state that "owning a website is analogous to owning a bookshop, the only party who can be said to purposely direct their acts towards a forum is the party who points his browser towards the website's landing page".[373] In other words, it is the customer, or the web user, that targets the shop, or the website, in order to use that particular service or to buy that specific item: "[t]he website owner has done nothing more than to set up a bookshop for others to direct themselves to and browse".[374]

The question that must be addressed is hence the following: is it sufficient that a non-EU company merely knows that its products may end up in the EU to trigger EU data protection legislation? Recital 23 of the GDPR offers some guidance in answering this question:

> In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is *apparent* that the controller or processor *envisages* offering services to data subjects in one or more Member States in the Union. Whereas the *mere accessibility* of the controller's, processor's or an intermediary's website in the Union, of an email address or of other *contact details*, or the use of a *language* generally used in the third country where the controller is established, is insufficient to ascertain such *intention*, factors such as the use of a *language* or a *currency* generally used in one or more Member States with the possibility of ordering goods and services *in that other language*, or the *mentioning* of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[375]

It is clear from this Recital that the "intention" of the controller or processor to target data subjects in the EU must be "apparent". This point was further clarified by the EDPB in its Guidelines on the territorial scope of the GDPR in which the EDPB stressed that "the provision is aimed at activities that intentionally, rather than inadvertently or incidentally, target individuals in the EU". This entails that if a company is offering goods or services to individuals outside the EU, but the service is not withdrawn once the individuals enter the EU, the processing activities related to that offer does not fall under the scope of application of the GDPR. Indeed, in "this case the processing is not related to the intentional targeting of individuals in the EU but relates to the targeting of individuals outside the

[373] de Hert and Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context," 241.

[374] Ibid.

[375] Recital 23 GDPR (italics mine).

EU which will continue whether they remain outside the EU or whether they visit the Union".[376] In the light of this, the second scenario presented above (i.e., a company wins customers in the EU market even though it does not actively endeavour to do so) does not seem to fall under the territorial scope of the GDPR.

Another question now arises: which factors *show the controller's intention* to target individuals in the EU? Some factors that may prove such an intent are listed in Recital 23 GDPR such as the use of a language or a currency that are generally used in the EU or the mentioning of customers or users in the EU. Certainly, in drafting Recital 23 GDPR, the EU co-legislators valued the clarifications given by the ECJ in the context of consumer protection law and in particular, in *Pammer and Hotel Alpenhof*,[377] where the ECJ was requested to establish "on the basis of what criteria a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Regulation No 44/2001, and second, whether the fact that those sites can be consulted on the internet is sufficient for that activity to be regarded as such".[378] The ECJ responded that

> in order to determine whether a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile, ..., it should be ascertained whether, before the conclusion of any contract with the consumer, it is *apparent* from those websites and the trader's overall activity that the trader was *envisaging* doing business with consumers domiciled in one or more

[376] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 15. The EDPB provides the following example: an "Australian company offers a mobile news and video content service, based on users' preferences and interest. Users can receive daily or weekly updates. The service is offered exclusively to users located in Australia, who must provide an Australian phone number when subscribing. An Australian subscriber of the service travels to Germany on holiday and continues using the service. Although the Australian subscriber will be using the service while in the EU, the service is not 'targeting' individuals in the Union, but targets only individuals in Australia, and so the processing of personal data by the Australian company does not fall within the scope of the GDPR".

[377] Judgment of 7 December 2010, *Pammer and Hotel Alpenhof*, Joined Cases C‑585/08 and C‑144/09, ECLI:EU:C:2010:740. For a detailed analysis of the principles established in *Pammer and Hotel Alpenhof*, see Dan Jerker B. Svantesson, "Pammer and Hotel Alpenhof – ECJ Decision Creates Further Uncertainty about When e-Businesses 'Direct Activities' to a Consumer's State under the Brussels I Regulation," *Computer Law & Security Review* 27, no. 3 (2011): 298–304.

[378] *Pammer and Hotel Alpenhof*, paragraph 47. This question concerned the correct interpretation of Article 15(1)(c) of Regulation No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters: "[i]n 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, jurisdiction shall be determined by this Section, without prejudice to Article 4 and point 5 of Article 5, if: … (c) in all other cases, the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, *directs* such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities" (italics mine).

> Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with them.[379]

As noted by the EDPB, even if the concept of "directing an activity" differ from the notion of "offering goods and services", the clarification given by the ECJ in *Pammer and Hotel Alpenhof* may help establish whether goods or services are intentionally offered to data subjects in the Union.[380]

The EDPB also identified some factors which may prove the non-EEA data controllers' intention to target individuals in the EU. Such factors should be taken in combination with one another so as to determine whether, overall, the commercial activities conducted by a non-EU data controller can be considered as offering goods or services directed at individuals in the EU. Such factors are, among others, the following:

- the international nature of the activity;
- the mention of addresses or phone numbers that can be reached from the EU;
- the mention of itineraries from EU Member States for going to the place where the service is provided;
- the use of a language or a currency other than the language or currency generally used in the trader's country and, in particular, the language or the currency of one or more EU Member State;
- the mention of an international clientele composed of customers domiciled in various EU Member States;
- the offer of a delivery of goods in EU Member States.[381]

The combination of these elements may hence provide evidence of the data controller's intention to target individuals in the EU while the processing activities of a data controller would fall outside the

[379] Ibid., paragraph 92 (italics mine).
[380] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 17.
[381] Ibid., 17–18.

territorial scope of the GDPR when goods or services are inadvertently offered to persons in the EU territory.[382]

In this context, the adoption of some technical solutions may also prevent companies from being caught under an "unwanted" jurisdiction. Geo-location technologies can, for example, be implemented in order to make explicit whether customers of a certain area are targeted or not. Indeed, geo-location technologies allow companies to pinpoint users' geographical location in order to tailor the content or to restrict access to the content of a website depending on the user's specific location. These technologies mainly fall under two categories: client-side and server-side. On the one hand, client-side geo-location technologies make use of users' computers or other wireless devices (e.g., smartphones, tablets) to establish their locations via a Global Positioning System (GPS) or the nearby wireless network towers. On the other hand, server-side geolocation technologies work remotely and retrieve users' location from their Internet Protocol (IP) addresses: geo-location tools acquire the IP address from the users and the geolocation provider compares that information with the information contained in a database that links IP addresses to a specific location.[383] By screening users by location, the implementation of such technologies can be interpreted as an indication of the *intention* of a company to avoid contact with the jurisdiction of a specific State or region.[384] In *UEJF et LICRA v. Yahoo! Inc. et Yahoo France*, for example, where Yahoo! was ordered by a French court to prevent

[382] Ibid., 18. The EDPB provides the following example: "A Swiss University in Zurich is launching its Master degree selection process, by making available an online platform where candidates can upload their CV and cover letter, together with their contact details. The selection process is open to any student with a sufficient level of German and English and holding a Bachelor degree. The University does not specifically advertise to students in EU Universities, and only takes payment in Swiss currency. As there is no distinction or specification for students from the Union in the application and selection process for this Master degree, it cannot be established that the Swiss University has the intention to target students from a particular EU member states. The sufficient level of German and English is a general requirement that applies to any applicant whether a Swiss resident, a person in the Union or a student from a third country. Without other factors to indicate the specific targeting of students in EU member states, it therefore cannot be established that the processing in question relates to the offer of an education service to data subject in the Union, and such processing will therefore not be subject to the GDPR provisions". Ibid., 19.

[383] Kevin F. King, "Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies," *Albany Law Journal of Science & Technology* 21 (2011): 66–67. See also, Dan Jerker B. Svantesson, "Time for the Law to Take Internet Geolocation Technologies Seriously," *Journal of private international law* 8, no. 3 (2012): 478–479.

[384] Dan Jerker B. Svantesson, "Geo-Location Technologies and Other Means of Placing Borders on the 'Borderless' Internet," *The John Marshall Journal of Computer and Information Law* 23, no. 1 (2004): 117.

French users from having access to Nazi memorabilia, the court deemed crucial in its holding the fact that Yahoo! had the technical ability to implement some forms of geographic control.[385]

Along this line of thinking, Svantesson suggested that the focus is shifted from "targeting" to "dis-targeting". Following this approach, companies should be required to take active steps to avoid contacts with customers/data subjects in a specific region in order *not* to be bound by the jurisdiction of that specific country. And the adoption of geo-location technologies could be one of the measures that would allow companies to refute "the presumption that they are targeting the world at large":[386] "[t]he 'dis-targeting' approach obligates businesses to actively regulate which jurisdictions they serve" and, hopefully, "whatever burden this present would be outweighed by the greater degree of predictability for liability".[387] However, it should also be noted that although the accuracy rates of such technologies are increasing, margins of error in the determination of the exact location of individuals ("source problems") are probably inevitable as well as attempts to circumvent geolocation technologies by individuals themselves, for example, by means of anonymising techniques or proxy servers ("circumvention problems").[388] Following the approach proposed by Svantesson – that is consistent with the approach adopted by the EDPB in its Guidelines on the territorial scope of the GDPR – if a company *happens* to sell goods/services to individuals in the European Union due to source problems or circumvention problems, it should be left immune from any legal responsibility under the GDPR if it is shown that the company has taken the steps available to avoid contact with individuals in the EU. Such steps may also include disclaimers that can be inserted on the website in

---

[385] *L 'Union Des Etudiants Juifs De France Et La Ligue Contre Le Racisme Et L 'Antisemitisme v. Yahoo! Inc. et Yahoo! France*, T.G.I. Paris, May 22, 2000, No. RG: 00/05308. See also, King, "Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies," 75–76; Marc H. Greenberg, "A Return to Lilliput: The LICRA v. Yahoo - Case and the Regulation of Online Content in the World Market," *Berkeley Technology Law Journal* 18, no. 4 (2003): 1217, https://scholarship.law.berkeley.edu/btlj/vol18/iss4/6. For a review of the cases where the existence of geo-location technologies has been taken into account in court, see Dan Jerker B. Svantesson, *Extraterritoriality in Data Privacy Law* (Copenhagen: Ex Tuto Publishing, 2013), 174–179.

[386] Svantesson, "Pammer and Hotel Alpenhof – ECJ Decision Creates Further Uncertainty about When e-Businesses 'Direct Activities' to a Consumer's State under the Brussels I Regulation," 303. See also, Dan Jerker B. Svantesson, "Delineating the Reach of Internet Intermediaries' Content Blocking - CcTLD Blocking, Strict Geo-Location Blocking or a Country Lens Approach," *SCRIPTed: A Journal of Law, Technology and Society* 11 (2014): 167.

[387] Svantesson, "Pammer and Hotel Alpenhof – ECJ Decision Creates Further Uncertainty about When e-Businesses 'Direct Activities' to a Consumer's State under the Brussels I Regulation," 303.

[388] Svantesson, *Extraterritoriality in Data Privacy Law*, 187–194.

order to explicitly specify that a particular product is not available for sale in a given State.[389]

As a further interpretative challenge, no distinction is made between companies that routinely target the EU market and those that only occasionally do so, meaning that companies that only occasionally offer services or goods to data subjects in the EU are also subject to the administrative burdens prescribed under the Regulation. However, it should be noted that a "relief" from these burdens is provided by Article 27(2)(a) GDPR. Indeed, the said Article prescribes that the obligation laid down in Article 27(1) – under which, "[w]here Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union" – does not apply to "processing which is *occasional*, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is *unlikely* to result in a *risk* to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing".[390]

3.4.4. The Application of the Monitoring Criterion

Article 3(2)(b) extends the applicability of the Regulation to the processing of personal data of data subjects who are in the European Union by a controller or a processor not established in the EU where the processing activities are related to the monitoring of the behaviour of those data subjects. The Regulation offers some guidance in interpreting this nexus by stating, in Recital 24, that

> [i]n order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are *tracked on the internet* including potential subsequent use of personal data processing techniques which consist of *profiling* a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.[391]

The European Parliament suggested to expand the understanding of monitoring activities for the purpose of the Regulation in order to cover "not only the monitoring of the behaviour of Union

[389] Svantesson, "Geo-Location Technologies and Other Means of Placing Borders on the 'Borderless' Internet," 123–124. See also, Bharat Saraf and Ashraf U. Sarah Sarah Kazi, "Analysing the Application of Brussels I in Regulating E-Commerce Jurisdiction in the European Union – Success, Deficiencies and Proposed Changes," *Computer Law & Security Review* 29, no. 2 (2013): 133.

[390] Article 27(2)(a) GDPR (italics mine).

[391] Recital 24 GDPR (italics mine).

residents by data controllers outside of the Union, such as through internet tracking, but all collection and processing of personal data about Union residents".[392] To this aim, in 2012, the European Parliament proposed to change the wording of Article 3(2)(b) from "the monitoring of their behaviour" to "the monitoring of such data subjects", and to expand the Recital proposed by the Commission[393] by specifying that in order to verify whether a processing activity can be considered as a form of monitoring it should be determined whether individuals are tracked not only on the Internet but also "through other means" and "if other data about them is collected, including from public registers and announcements in the Union that are accessible from outside of the Union".[394] A similar attempt to expand the scope of monitoring is also witnessed by the amendments proposed by the European Parliament in its 2014 Position Paper where, among other things, it proposed the deletion of "the internet" as a means for tracking:

[392] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 63.

[393] Recital 21, European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 20.

[394] Recital 21, European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 14–15.

2012 Proposal of the European Commission[395]	2012 Draft Report of the European Parliament[396]	2014 Position Paper of the European Parliament[397]
Recital 21: In order to determine whether a processing activity can be considered to 'monitor **the behaviour' of** data subjects, it should be ascertained whether individuals are tracked **on the internet with** data processing techniques which consist of applying a 'profile' **to an individual**, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	Recital 21: In order to determine whether a processing activity can be considered to 'monitor' data subjects, it should be ascertained whether individuals are tracked on the internet **or through other means**, **or if other data about them is collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of** data processing techniques which consist of applying a 'profile', particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	Recital 21: In order to determine whether a processing activity can be considered to 'monitor ~~the behaviour'~~ of data subjects, it should be ascertained whether individuals are **tracked ~~on the internet with~~, regardless of the origins of the data, or if other data about them are collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of** data processing techniques which consist of applying a 'profile' ~~to an individual~~, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

Table 4 – Development of the monitoring criterion

The European Parliament's suggestions were, however, not incorporated in the final text, which, rather, compared to the original proposal includes the addition "as far as their behaviour takes place within the European Union". At the same time, the EDPB has clarified that even if Recital 24 GDPR only refers to the monitoring of a person through the tracking of a person on the Internet, "tracking through other types of network or technology involving personal data processing should also be taken into account in determining whether a processing activity amounts to a behavioural monitoring, for example through wearable and other smart devices".[398]

Moreover, the EDPB has noted that, unlike Article 3(2)(a) GDPR and Recital 23 GDPR, neither Article 3(2)(b) nor Recital 24 GDPR specifically refer to the intention to target. At the same

[395] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*.

[396] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*.

[397] Recital 21, European Parliament, *Position of the European Parliament Adopted at First Reading on 12 March 2014 with a View to the Adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (EP-PE_TC1-COD(2012)0011)*, 2014, 12, accessed April 16, 2018, https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TC+P7-TC1-COD-2012-0011+0+DOC+PDF+V0//EN.

[398] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 19.

time, however, "the use of the word 'monitoring' implies that the controller has a specific *purpose in mind for the collection and subsequent reuse* of the relevant data about an individual's behaviour within the EU".[399] This entails that, in order to determine whether a non-EU data controller falls within the territorial scope of the GDPR, it is necessary "to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data".[400] The EDPB has further provided some examples of the processing activities which may be caught under the scope of article 3 GDPR:

- Behavioural advertisement
- Geo-localisation activities, in particular for marketing purposes
- Online tracking through the use of cookies or other tracking techniques such as fingerprinting
- Personalised diet and health analytics services online
- CCTV
- Market surveys and other behavioural studies based on individual profiles
- Monitoring or regular reporting on an individual's health status.[401]

It is clear from this list that, even though the EDPB has stressed that not any online collection and analysis of personal data would amount to "monitoring",[402] the range of monitoring activities that may fall under the scope of the GDPR remains extremely broad.

In particular, the fact that online tracking through the use of cookies is also included in this list may revive the undesirable consequence of "a possible universal application of EU law"[403] that has been identified by A29WP with reference to the equipment criterion. When it comes to the use of tracking tools which operate on the use of cookies or similar applications, a perfect correspondence can, indeed, be traced between the applicability of Article 4(1)(c) of the 1995 Directive and Article 3(2)(b) of the Regulation. Let's take the example of an individual that is using her/his own personal computer in the EU and accesses a US website that is making use of cookies. This scenario falls squarely within the scope of Article 4(1)(c) of the 1995 Directive: 1) the data controller is not established in the European Union; 2) the data controller is making use of an equipment (the personal

[399] Ibid., 20 (italics mine).
[400] Ibid.
[401] Ibid., 20.
[402] Ibid.
[403] Article 29 Data Protection Working Party, *WP179*, 31.

computer of the data subject) by means of cookies for the purpose of processing personal data. At the same time, the same scenario would trigger the application of the Regulation under Article 3(2)(b): 1) the data controller is not established in the European Union; 2) the processing activities conducted by the data controller are related to the monitoring of the behaviour of the data subject by means of cookies; 3) the (surfing) behaviour of the data subject takes place in the European Union. In other words, any company with an online presence would be at risk of being exposed to the strict obligations set out under the EU data protection legislation as soon as they come into contact with individuals in the European Union.[404] To make things worse, the EDPB's Guidelines do not clarify whether monitoring only covers activities *over a period of time*. In the absence of this clarification, even "'instant' and 'snapshot' activities" may trigger the application of the GDPR.[405]

3.4.5. What Has Changed, and What Has Not?

The potential (over)broad application of both the equipment criterion and the targeting and monitoring criteria is undisputed. As a subtle difference, it can be noted that while the equipment criterion seems to derive its broad application mainly from the extensive interpretation to which it has been subject, the broad application of Article 3(2) of the Regulation seems to have been specifically intended by the EU co-legislators. Several grey areas and legal uncertainties certainly remain: the uncertainties revolving around the definition of the equipment have, indeed, been replaced with uncertainties revolving around the interpretation and application of the targeting test and the definition of monitoring activities.

Overall, however, the shift from the equipment criterion (and hence from the territoriality principle) to the monitoring and targeting criteria (and hence to the passive personality principle), should be applauded, at least from a theoretical viewpoint. Firstly, the targeting and the monitoring

[404] Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," 74.

[405] Centre for Information Policy Leadership, *Comments on the European Data Protection Board's "Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)" Adopted on 16 November 2018*, 16.

of data subjects in the EU seem to provide a stronger connection to the EU compared to the equipment criterion. Indeed, the targeting and the monitoring criteria seem to impose additional burdens on data controllers (and processors) in taking positive steps to direct their activities to individuals in the EU while equipment in the EU could also be used to process personal data about data subjects outside the European Union. Secondly, the focus on the data subject ("data subjects who are in the Union") rather than on the equipment deployed for data processing is more consistent with the ultimate goal of the Regulation, i.e., strengthening the protection of the individuals' fundamental right to personal data. Thirdly, the adoption of a criterion already endorsed in the field of consumer protection law, i.e., the targeting approach, entails that data controllers (and processors) may benefit not only from clarifications and advances made in the data protection field, but also from those made in consumer protection law, thus increasing legal certainty. As noted by A29WP back in 2010, "applying [the targeting criterion] in a data protection context would bring additional legal certainty to controllers as they would have to apply the same criterion for activities which often trigger the application of both consumer and data protection rules".[406]

The replacement of the equipment criterion with the "offering of goods or services" and the "monitoring" criteria has also been welcomed by the European Data Protection Supervisor who noted that "the offering of goods and services or the monitoring of the behaviour of data subjects in the Union makes much more sense and is more in line with the reality of global exchanges of information than the existing criterion of the use of equipment in the EU".[407]

3.5. Nexus 3: The Application of the GDPR to the Processing of Personal Data in a Place Where Member State Law Applies by Virtue of Public International Law

Under Article 3(3) GDPR, the "Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law". Article 3(3) of the Regulation refers to situations where, under public

[406] Article 29 Data Protection Working Party, *WP179*, 31.

[407] European Data Protection Supervisor, *Opinion on the Data Protection Reform Package*, 2012, 17, accessed November 30, 2019, https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

international law, EU law, including EU data protection law, applies to embassies and consulates of EU Member States abroad[408] as well as ships or airplanes flying the flag of a Member State or to embassies, consulates of EU Member States abroad.[409] This is also confirmed by Recital 25 of the Regulation: "[w]here Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post".[410] Since this nexus only applies to some limited situation, it lacks of strong practical significance. However, the relevance of this criterion may increase with the emergence of underwater and floating data centres such as those being developed, for example, by Microsoft[411] and Google.[412]

It is worth highlighting that, although the EU co-legislators have formulated Article 3(3) of the Regulation by using the same wording of Article 4(1)(b) of the 1995 Directive, the "order" of the nexuses has been changed under the Regulation:

1. Directive: 1. establishment (Art.4(1)(a)) → **2.** *public international law* (Art.4(1)(b)) → 3. equipment (Art.4(1)(c)).
2. Regulation: 1. establishment (Art.3(1)) → 2. targeting or monitoring (Art.3(2)) → **3**. *public international law* (Art.3(3)).

---

[408] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 22.

[409] Article 29 Data Protection Working Party, *WP179*, 18. See also, Hon, Hörnle, and Millard, "Which Law(s) Apply to Personal Data in Clouds?," 227.

[410] Recital 25 GDPR.

[411] Among others, Athima Chansanchai, "Microsoft Research Project Puts Cloud in Ocean for the First Time," *Microsoft Stories*, February 1, 2016, accessed April 7, 2018, https://news.microsoft.com/features/microsoft-research-project-puts-cloud-in-ocean-for-the-first-time/; Yevgeniy Sverdlik, "Microsoft Wants to Patent an Underwater Data Center," *Data Center Knowledge*, last modified January 9, 2017, accessed April 7, 2018, http://www.datacenterknowledge.com/archives/2017/01/09/microsoft-wants-to-patent-an-underwater-data-center-reef; John Markoff, "Microsoft Plumbs Ocean's Depths to Test Underwater Data Center," *The New York Times*, January 31, 2016, accessed April 7, 2018, https://www.nytimes.com/2016/02/01/technology/microsoft-plumbs-oceans-depths-to-test-underwater-data-center.html; John Roach, "Under the Sea, Microsoft Tests a Datacenter That's Quick to Deploy, Could Provide Internet Connectivity for Years," *Microsoft*, last modified June 5, 2018, accessed November 24, 2019, https://news.microsoft.com/features/under-the-sea-microsoft-tests-a-datacenter-thats-quick-to-deploy-could-provide-internet-connectivity-for-years/.

[412] Among others, Rich Miller, "Google Gets Patent for Data Center Barges," *Data Center Knowledge*, last modified April 29, 2009, accessed April 7, 2018, http://www.datacenterknowledge.com/archives/2009/04/29/google-gets-patent-for-data-center-barges; Rory Carroll, "Google's Worst-Kept Secret: Floating Data Centers off US Coasts," *The Guardian*, October 30, 2013, accessed April 7, 2018, http://www.theguardian.com/technology/2013/oct/30/google-secret-floating-data-centers-california-maine.

Under the DPD, the A29WP suggested that the steps that had to be followed in order to determine whether the EU jurisdiction was triggered had to reflect the order offered by the EU co-legislators:

1. Does the controller have an establishment in one or more Member States (Art.4(1)(a))? If not, proceed with step 2.
2. *Is the controller established at a location where the national law of the Member State is applicable by virtue of public international law* (Art.4(1)(b))? If not, proceed with step 3.
3. Does the controller use equipment that is located in a Member State (Art.4(1)(c))? If not, the national law of the Member State implementing the 1995 Directive is not applicable.[413]

The same logic could be applied to the Regulation, so that the applicability of the EU data protection provisions by virtue of public international law could be left as a third, residual, possibility:

1. Does the controller or the processor have an establishment in the European Union (Art.3(1))? If not, proceed with step 2.
2. Are the processing activities of personal data of data subjects who are in the European Union by a controller or a processor related to the offering of goods or services or the monitoring of their behaviour (Art.3(2))? If not, proceed with step 3.
3. *Is the controller established at a location where the national law of the Member State is applicable by virtue of public international law* (Art.3(3))? If not, the Regulation is not applicable.

3.6. The (Undesirable) Consequences of the Unilateral Expansion of the EU Jurisdiction

Cross-border activities need laws designed to cross traditional geographical borders. A flexible approach to the territorial scope may make legislation fit for the transnational processing

[413] Annex, Article 29 Data Protection Working Party, *WP179*. The A29WP's suggestion to leave the equipment criterion as a third possibility, where the two other grounds for jurisdiction do not apply, was mainly driven by the necessity to limit, to the extent possible, its "undesirable consequences": "[t]he equipment/means criterion could therefore be kept, in a fundamental rights perspective, and in a residual form. It would then only apply as a third possibility, where the other two do not: it would address borderline cases (data about non EU data subjects, controllers having no link with EU) where there is a relevant infrastructure in the EU, connected with the processing of information". Ibid., 31–32.

operations of the fast-moving digital age.[414] The need to adapt the criteria that are traditionally deployed to determine States' jurisdictions to todays' global phenomena has emerged not only in the EU data protection framework but also in other areas of law where the ECJ and other EU institutions have tried to "adjust" existing rules to the challenges raised by the increasingly interconnected and globalized world in which we live. The need to extend the reach of EU law to conducts originating in third countries generally respond to the need to ensure the effectiveness of EU rules especially when those rules aim to protect public policy interests as is surely the case with the fundamental right to data protection (3.2.2.).[415] Nonetheless, as the analysis above has shown, the (over)broad (extra)territorial claims made by the EU co-legislators via the 1995 Directive first, and the Regulation after, may undermine the very objective of EU data protection legislation: *effective* protection of fundamental rights in general, and right to privacy in particular.

Firstly, conflicts of law are an inevitable consequence of the unilateral expansion of jurisdiction across borders. In the absence of mutual agreements, the extraterritorial application of the EU data protection legislation leads to the (potential) simultaneous application over the same facts/actions of conflicting legal rules dictated by different States that are all interested in preserving their jurisdiction in the presence of (some) connecting factors.[416] Uncertainty about the applicable rules clearly compromise the right for companies and individuals operating outside the European Union to know to which legal provisions they are subject. Processors and controllers outside the EU may, in fact, be trapped in a network of conflicting rules all resting on different possible legitimate

[414] de Hert and Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context," 239.

[415] Taylor (2015) argues that there is a causality between the evolution of data protection from economic necessity to an autonomous fundamental right on the one hand and the (extra)territorial extension of EU law to protect this right on the other: "[a]s the fundamental right to data protection morphs to carry more weight in the EU, this could amplify the EU's obligations under human rights law to protect its citizens' personal data when such data are processed outside EU territory". Mistale Taylor, "The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect," *International Data Privacy Law* 5, no. 4 (November 1, 2015): 255–256. See also Jääskinen and Ward, "The External Reach of EU Private Law in the Light of L'Oréal versus EBay and Google and Google Spain," 144–145; *The Internet and the Global Reach of EU Law* (LSE Law, Society and Economy Working Papers 4/2017 - University of Cambridge Faculty of Law Research Paper No. 24/2017, 2017), 21, accessed June 6, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890930.

[416] de Hert and Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context," 239.

triggers (e.g., nationality, territoriality, effects) thus putting them in a confusing and excessively burdensome position, especially when penalties for non-compliance are high.[417] In this overwhelming framework, non-EU companies may just choose not to comply with the requirements under the GDPR (especially in the light of the enforceability problems that will be discussed below), not to mention that companies may also be unaware of their compliance duties considering the uncertainties that still affect the key terms of Article 3 GDPR. Interestingly, the problems that may arise from these conflicts of law have been acknowledged by the European Parliament in the position it adopted at first reading on 12 March 2014. Unsurprisingly, the solution proposed the European Parliament in case of conflicting compliance requirements is, simply, that EU law "takes precedence at all time":

> In cases where controllers or processors are confronted with conflicting compliance requirements between the jurisdiction of the Union on the one hand, and that of a third country on the other, the Commission should ensure that Union law takes precedence at all times. The Commission should provide guidance and assistance to the controller and processor, and it should seek to resolve the jurisdictional conflict with the third country in question.[418]

Secondly, problems of enforceability inevitably accompany the extraterritorial application of the Regulation. Investigations and enforcement actions relating to activities conducted by foreign companies with no physical presence in the European Union and where only a loose connection with the EU can be identified, are bound to face several legal, administrative and practical obstacles. Despite the broad extraterritorial claims made under the Regulation, the actual enforcement of its provisions is hence likely to be limited to the bigger actors that have a strong impact on the EU market.[419] In this regard, some have noted that similar enforceability problems are outweighed by the symbolic value of extraterritorial claims. Indeed, assuming that companies generally prefer not to

---

[417] Ibid., 240.

[418] Recital 90, European Parliament, *Position of the European Parliament Adopted at First Reading on 12 March 2014 with a View to the Adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (EP-PE_TC1-COD(2012)0011)*, 65.

[419] Svantesson, "Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation," 232. At the same time, there is evidence that enforcement actions may also be taken against companies that are located outside the EU. For example, the Information Commissioner's Office (ICO), i.e., the UK Data Protection Authority, has adopted two enforcement notices against AggregateIQ Data Services Ltd, a Canadian company with no physical presence in the EU accused of unlawfully processing data of individuals in the UK for Brexit campaigns. See ICO's enforcement notice, July 6, 2018, accessed November 23, 2019, https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf, and ICO's enforcement notice, October 24, 2018, accessed November 23, 2019, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf.

engage in activities that may turn out illegal, extraterritorial claims may have an important deterrent effect for foreign companies.[420] Sanctions for non-compliance may also have a substantial reputational impact on companies, especially on those which are more exposed to the public opinion.[421] This is what Svantesson has labelled "bark jurisdiction", i.e., "jurisdictional claims ... that have virtually no prospect of being exercised in reality", as opposed to "bite jurisdiction".[422] Despite their weak grip on reality, Svantesson recognized the importance of such claims since they allow States to signal to the international community their attempts to grant an effective protection of the right to privacy and hence to assert the international legitimacy of such attempts:[423] "it could be said that 'bark jurisdiction' signals a perceived right to regulate a particular matter while acknowledging the lack of ability to regulate that matter".[424]

However, Svantesson himself acknowledged that "the jurisdictional claims made in Article 3 of the proposed Regulation (as well as in Article 4 of the...Directive) are too wide, and some of the substantive rules (eg the requirement of a data protection officer) too burdensome to be viewed as legitimate bark jurisdiction".[425] After all, "[t]he applicability of law to conduct, or the adjudication of a dispute by a court or regulator, is not a purely theoretical matter, but must have a reasonable

[420] Ibid., 233. Along the same lines, de Hert and Czerniawski (2016) noted that "[t]here might be a serious problem with enforceability ..., but the interests at stake are very high and the extension of scope seems fully justified". de Hert and Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context," 240.

[421] Adèle Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 9, no. 2 (2018): 135, accessed April 19, 2019, https://www.jipitec.eu/issues/jipitec-9-2-2018/4723/JIPITEC_9_2_2018_126_Azzi. See also, Robert Madge, "GDPR's Global Scope: The Long Story," *MyData Journal*, May 12, 2018, accessed April 12, 2019, https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f.

[422] Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," 58–59. The same concept was expressed by Bygrave (2000) when he highlighted that the equipment criterion may lead to a "regulatory overreaching in an online environment". "By 'regulatory overreaching' is meant a situation in which rules are expressed so generally and non-discriminatingly that they apply prima facie to a large range of activities without having much of a realistic chance of being enforced". Lee A. Bygrave, "European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation," *Computer Law & Security Review* 16, no. 4 (August 1, 2000): 255.

[423] Svantesson, "Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation," 233.

[424] Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," 60.

[425] Svantesson, "Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation," 233.

chance of enforcement in order to have meaning".[426] Meaningless forms of jurisdiction may instead undermine the general respect for data protection law.[427] A similar argument was also proposed by Reed (2013) when he stated that enforcement is an essential component of the legitimacy of a governance system: "[a] regulator which is...accepted as having legitimate authority can easily lose that authority if it has no effective way of enforcing its rules. Conversely, a regulator which achieves a high level of compliance will enhance its legitimacy".[428]

This (likely) gap between applicability and enforceability suggests that the balance between legal certainty and flexibility on which the current wording of the territorial scope is based should be revisited so as to tilt the scale more on legal certainty and a bit less on flexibility. A more "cautious" or, we could say, "reasonable" approach could hence be adopted in interpreting and applying the law.[429] As preached (but not practiced) by the A29WP in WP56, the EU data protection rules should apply only "where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved".[430] As stressed by Kuner (2015), enforcement actions are the tool that has the greatest effect on influencing the behaviours of commercial actors.[431] By ensuring that the application of the EU data protection legislation is strongly linked to enforceability and, consequently, by increasing the risk for companies of facing enforcement actions, the overall level of compliance with the applicable legislation – both within and outside the EU – could be increased.

The EDPB itself seems to be well aware of these enforceability problems on non-EU data controllers since the "enforcement against controllers in [third] countries" was included among the

[426] Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)," *International Journal of Law and Information Technology* 18, no. 3 (2010): 236.

[427] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 125.

[428] Chris Reed, "Cloud Governance: The Way Forward," in *Cloud Computing Law* (Oxford: Oxford University Press, 2013), 374.

[429] Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)," 244–245.

[430] Article 29 Data Protection Working Party, *WP56*, 9.

[431] Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law," 244–245.

possible topics of EDPB Work Program 2019/2020.[432] At the same time, it could be argued that some of the enforceability problems that have been analysed above may be (partially) solved by the obligation to appoint a representative within the EU, obligation that Article 27 GDPR imposes on controllers and processors which are not established in the EU and which are subject to the GDPR by virtue of Article 3(2) GDPR. The appointment of a representative in the EU is, indeed, meant to ensure that data subjects and the DPAs in the EU can easily connect with the non-EU data controller or processor. As stressed by the EDPB, the concept of representative was introduced so as to ensure an easy dialogue between non-EU entities and EU data subjects and DPAs, including effective enforcement against controllers and/or processors which would otherwise be out of reach for the EU DPAs. DPAs can hence initiate enforcement actions against non-EU controllers/processors *through* their EU representatives. This entails that, enforcement actions can be *addressed* to the EU representatives even though such actions are *directed* to the non-EU data controller or processor they represent. At the same time, EU representatives shall not be held directly liable for any misdemeanour committed by the non-EU entity. In this regard, the EDPB has clarified that the "GDPR does not establish a substitutive liability of the representative in place of the controller or processor it represents in the Union".[433] The "possibility to hold a representative directly liable is ... limited to its *direct* obligations referred to in articles 30 and article 58(1) a of the GDPR"[434] (i.e., the obligation to keep a record of processing activities and to provide to DPAs any information required).

3.7. Conclusion

The *extra*-territoriality of the GDPR has become a buzzword. However, the analysis conducted above has shown that several uncertainties still affect a clear understanding of this concept. Indeed, Article 3 of the Regulation is likely to both perpetuate some uncertainties that have already

[432] European Data Protection Board, *Work Program 2019/2020*, 2019, accessed January 6, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf.

[433] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 27.

[434] Ibid., 28 (italics mine).

emerged under the 1995 Directive and raise new ones. These uncertainties may compromise the very objective of achieving a harmonized data protection framework, which stands behind the decision to resort to a regulation rather than to a directive.[435]

With reference to nexus 1, the uncertainties that have emerged under the 1995 Directive are likely to continue to haunt the Regulation since the key words of Article 4(1)(a) DPD ("establishment", "in the context of the activities of an establishment") are not only transposed in Article 3(1) of the Regulation but also extended to processors, which become directly subject to the EU legislation. Indeed, processors may fall directly under the scope of the GDPR even when the controller on behalf of which they process data is not subject to the Regulation. This brings some unreasonable and unpractical consequences such as the duty to enter into a DP Agreement with the non-EU data controller even if that controller is not subject to the GDPR. As for nexus 2, the removal of the equipment criterion (Article 4(2)(c) DPD) and its replacement with the targeting and the monitoring criteria (Article 3(2) of the Regulation) should be applauded. Nonetheless, on the one hand, the targeting test would certainly benefit from further clarifications, considering the practical difficulties that may emerge in determining the subjective intention of a company offering goods or services to data subjects in the EU; on the other hand, the monitoring criterion may revive the "undesirable" consequence of a "possible universal application of EU data protection law".[436] The conflicts of law and the enforceability problems that may derive from this unilateral expansion of the EU jurisdiction have also been analysed. To address these problems, a more cautious approach in interpreting and applying Article 3 was suggested in order to fill the gap between applicability and enforceability of the EU legislation.

[435] The decision to resort to a regulation was triggered by the necessity to put an end to the fragmented legal environment – and the legal uncertainties and unequal levels of protection for the data subjects – that resulted from the diverse implementation of the 1995 Directive across the EU. Indeed, while EU directives set out a scope that Member States must achieve and then leave it to the discretion of each country to decide how to reach it, EU regulations are binding legislative acts that are directly applicable across the EU in the way they are presented. The adoption of a regulation was hence seen as the most suitable means for replacing the patchwork of different laws developed under the 1995 Directive with a harmonized data protection framework throughout the European Union.

[436] Article 29 Data Protection Working Party, *WP179*, 31.

The next chapter will start delving into the EU data transfer rules, firstly, by focusing on the reasons that underpin such rules and, secondly, by investigating how the very concept of "transfer" has been interpreted and defined within the European Union by the EU courts and by EU Member States' legislation and data protection authorities. Some inconsistencies between the jurisdictional grounds prescribed under Article 3 GDPR and the rules that limit the transfer of personal data outside the EU under Chapter V GDPR will start to emerge: on the one hand, as seen above, jurisdictional rules disregard data location, on the other hand, data transfer rules revolve entirely around data location.

4. Restrictions to International Data Transfer: Untangling the Concept of Transfer

4.1. Introduction

Chapter IV of the 1995 Directive deals with the "Transfer of personal data to third countries". Its counterpart in the Regulation is Chapter V that regulates the "Transfer of personal data to third countries or international organisations". Under the said chapters, transfer of data to third countries and, under the GDPR, also to international organisations is prohibited unless a number of conditions is met. As it was prescribed under the 1995 Directive, compliance with such conditions is an additional requirement that goes on top of other requirements prescribed by the GDPR. Transfer of data is, indeed, a form of processing that will also be subject to the other provisions of the Regulation. This is made explicit under Article 44 of the Regulation that clarifies that transfer of data "shall take place only if, subject to the *other provisions* of this Regulation, the conditions laid down in ... Chapter [V] are complied with by the controller or processor".[437] It is also worth stressing that under both the 1995 Directive and the Regulation, data export restrictions only concern transfer of data to non-EEA countries while the movement of personal data within the EU shall not be restricted or prohibited for data protection reasons. Indeed, the objective of the 1995 Directive, that has now been transposed to the Regulation, was not only to ensure high and harmonized standards of data protection across the European Union but also to facilitate the intra-EU free flow of data as a precondition for achieving the EU Digital Single Market.[438] The aim of this chapter is to analyse the very basics of data transfer

[437] Article 44 GDPR (italics mine). Article 25(1) of the 1995 Directive included a similar provision: "[t]he Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, *without prejudice* to compliance with the national provisions adopted pursuant to the *other provisions* of this Directive, the third country in question ensures an adequate level of protection" (italics mine). On this ground, transfer, as any other form of processing of data, is lawful only to the extent that at least one of the grounds for data processing prescribed under Article 6 GDPR ("Lawfulness of processing") applies. Similarly, by virtue of Article 5 GDPR ("Principles relating to processing of personal data"), data shall not be transferred (i.e., "further processed") "in a manner that is incompatible with" the purpose for which they have been originally collected.

[438] Article 1 1995 Directive: "1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1". See also Recitals 3 and 8 of the 1995 Directive. Article 1(3) GDPR reiterates that "[t]he free movement 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". Similarly, Recital

provisions so as to unveil not only the reasons why international data transfer is restricted but also, in the absence of an official definition, the very understanding of the concept of "transfer".

4.2. The Underlying Objective(s) of Data Export Restrictions

4.2.1. Anti-circumvention Objective

The risk of circumvention of the law is frequently mentioned as the main policy objective underpinning data export restrictions. Indeed, as seen above (2.3), restrictions to transborder data flow have been mainly driven by the fear that national laws could be circumvented if data are moved to jurisdictions with lower standards of protection. The fear of circumvention is clearly underpinning the barriers to data transfer set out in the 1980 OECD Guidelines and in Convention 108 (and its 2001 Additional Protocol)[439] on the premises of which the 1995 Directive (and hence also the Regulation) has been built. Indeed, under paragraph 17 of the 1980 OECD Guidelines, a Member country should refrain from imposing barriers to data transfer between itself and another Member country "except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would *circumvent* its domestic privacy legislation".[440] The Explanatory Memorandum of the Guidelines clarifies that transborder data flow can be legitimately restricted, for example, in order to oppose "attempts to circumvent national legislation by processing data in a Member country which does not yet substantially observe the Guidelines". At the same time, the Explanatory Memorandum also clarifies that such restrictions to transborder data flow are not justified when the country to which data are transferred provides protection which is "substantially similar in effect to that of the exporting country", yet not identical. In other words, the 1980 OECD Guidelines establish "a standard of equivalent" – which does not mean identical – "protection".[441] This approach is confirmed in the

13 GDPR states that "[i]n order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the *free movement* of personal *data within the internal market*, a Regulation is necessary to provide legal certainty and transparency for economic operators" (italics mine). See also Recital 123 GDPR.

[439] 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* (Strasbourg: ETS No. 181, 2001), (hereafter cited as Additional Protocol to Convention 108).

[440] Paragraph 17, 1980 OECD Guidelines (italics mine).

[441] Paragraph 17, *Explanatory Memorandum*, 1980 OECD Guidelines.

2013 revised version of the OECD Guidelines which provide, under paragraph 17, that a Member State should not restrict international data flow when "the other country substantially observes these Guidelines".[442]

Along the same lines, Article 12 of Convention 108 provides that "[a] Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party".[443] The said article hence establishes the principle of free flow of data between the Parties to the Convention. The transfer of personal data to recipients which are *not s*ubject to the jurisdiction of a Party to the Convention is also indirectly addressed since Article 12(3) provides that a Party is entitled to restrict data transfer when "the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, *in order to avoid such transfers resulting in circumvention of the legislation*" of the exporting country.[444] Article 2 of the Additional Protocol to the Convention has further strengthened the guarantees established under Convention 108 by specifically regulating the transfer of personal data from a contracting State to a "recipient which is not subject to the jurisdiction of a Party to the Convention". In particular, Article 2 provides that "[e]ach Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures *an adequate level of protection* for the intended data transfer".[445] In other words, the transfer of personal data to a recipient which does not fall under the jurisdiction of a Party to the Convention is subject to the condition that the recipient country or organization affords *an adequate level of protection*.[446]

---

[442] Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 16 (paragraph 17).

[443] Article 12, Convention 108.

[444] Article 12, Convention 108 (italics mine).

[445] Article 2, Additional Protocol to Convention 108 (italics mine).

[446] Council of Europe, *Explanatory Report to the 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* (Strasbourg: ETS No. 181, 2001), paragraph 25.

A similar provision is retained and expanded under the modernized version of the Convention, which was revised in 2018 so as to address the new challenges of the digital era[447] (Convention 108 +). Indeed, besides reaffirming the principle of free flow of personal data from a Party to the Convention to another Party to the Convention (or better, to a recipient who is subject to the jurisdiction of another contracting State), Article 14 of Convention 108 + provides that when "the *recipient* is subject to the jurisdiction of a State or international organisation *which is not Party to this Convention,* the transfer of personal data may only take place where *an appropriate level of protection* based on the provisions of this Convention is secured".[448] The explanatory report of the Protocol Amending Convention 108 makes the anti-circumvention purpose of data transfer rules even more explicit:

> The purpose of the transborder flow regime is to ensure that personal data originally processed within the jurisdiction of a Party (data collected or stored there, for instance), which is subsequently under the jurisdiction of a State which is not Party to the Convention, *continues* to be *processed* with *appropriate safeguards*. What is important is that data processed within the jurisdiction of a Party always remains protected by the relevant data protection principles of the Convention.[449]

It is hence clear that the aim of data transfer rules is to ensure that the level of protection afforded by a contracting State is not undermined once data leave the State. Appropriate safeguards should hence be implemented so as to ensure that the data protection principles of the Convention "follow" the data even when the data leave the borders of a contracting State.

The same concerns about the circumvention of the law stands behind the data export restrictions set out under the 1995 Directive and the GDPR. Such concerns were made explicit back in 1992 in the Amended Proposal for the Directive: "[t]he rule intended to prevent the Community rules from being *circumvented* in the course of transfers of data to non-community countries takes

---

[447] Council of Europe, *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Strasbourg: CETS No. 223, 2018). The consolidated version of Convention 108+ is available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[448] Article 14, Convention 108 + (italics mine).

[449] Council of Europe, *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Strasbourg: CETS No. 223, 2018), paragraph 103 (italics mine).

the form of a *ban* on the *transfer* of data to countries which do not provide an adequate level of protection".[450] The anti-circumvention purpose of the data export restrictions was also highlighted by the A29WP in 1995:

> ... [T]he rationale of the principle of adequate protection, enshrined in Article 25, consists in ensuring that individuals should continue to benefit from the fundamental rights and freedoms which they are granted in relation to the processing of their data in the European Union once these data have been transferred to a third country. It also aims at preventing that the protection provided by European personal data protection legislation be circumvented by the fact of transferring the data to third countries.[451]

Moving to the case law, and more recently, in *Schrems*, the ECJ noted that "the high level of protection guaranteed by Directive 95/46 read in the light of the [EU Charter of Fundamental Rights] could easily be *circumvented* by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries".[452]

The anti-circumvention objective now clearly emerges from Article 44 of the GDPR, where it is stated that all provisions about transfer of data outside the EU "shall be applied in order to ensure that the *level of protection* of natural persons guaranteed by this Regulation is *not undermined*".[453] Notably, the GDPR explicitly acknowledges that circumvention risks arise not only in case of transfer but also in case of onward transfer.[454] In its 2017 communication to the European Union on "Exchanging and Protecting Personal Data in a Globalised World", the European Commission also stressed that the "primary purpose of these rules is to ensure that when the personal data of Europeans are transferred abroad, the protection travels with the data".[455] In the light of the above, it can be

---

[450] Commission of the European Communities, *Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 4 (italics mine).

[451] 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)*, 2005, 6–7, accessed December 8, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf.

[452] Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 73 (italics mine).

[453] Article 44 GDPR (italics mine).

[454] Article 44 GDPR, in fact, prescribes that the provisions about international data transfer shall also be complied with in the event of "onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation". Consistently, Recital 101 GDPR provides that "when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, *including in cases of onward transfers* of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation" (italics mine).

[455] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 4.

safely concluded that data export restrictions set out under the DPD before and under the GDPR now are (mainly) motivated by the fear that transfer of data to non-EEA countries could lead to the circumvention of the principles established under the EU data protection legislation.

4.2.2. Preventing Access by Foreign Public Authorities

Besides the attempt to avoid the circumvention of the EU data protection rules, another policy objective seems to have motivated the adoption of data transfer rules: the need to protect personal data from foreign public authorities. This (second) objective derives from the fact that while, under the EU legislation, data protection principles can be subject to restrictions only when such restrictions respect "the essence of the fundamental rights and freedoms and [are] a necessary and proportionate measure in a democratic society to safeguard", among others, national security and other objectives of general public interest,[456] when data are transferred to third countries, such data may be exposed to public interventions that infringe upon the essence of the fundamental rights and freedom and that go beyond what is necessary in a democratic society. This concern emerges from Recital 116 GDPR that states that "[w]hen personal data moves across borders *outside* the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the *unlawful* use or *disclosure* of that information".[457]

The fear that data located in "insecure" third countries may be more "exposed" to disclosure requests (or direct seizure) by foreign public authorities resonates in several A29WP's opinions. Back in 1998 (WP12), the A29WP identified the "problem of overriding law" as one of the major limitations of the use of contracts as a legal basis for data transfer (5.5.1.1.). The legal framework of a third country may, indeed, require the recipient in that third country to disclose personal data to public authorities and these disclosure requests inevitably take precedence over the contract signed between the data exporter and the data recipient:

[456] Article 23 GDPR. A similar provision was prescribed under Article 13 of the 1995 Directive ("Exemptions and restrictions").

[457] Recital 116 GDPR (italics mine).

> under the directive any such disclosures (which are by their nature for purposes incompatible with those for which the data were collected) must be limited to those necessary in democratic societies for one of the 'ordre public' reasons set out in Article 13(1) of the directive... In third countries similar limitations on the ability of the state to require the provision of personal data from companies and other organisations operational on their territory may not always be in place.[458]

Consistently, in 2001 (WP47), the A29WP highlighted that one of the main differences between processors established inside the EU and processors established outside the EU is that "there is always the possibility of data processors in third countries being subject to *public interventions* which might go *beyond* what is *necessary* in a *democratic society*".[459] Likewise, in 2014 (WP228), the A29WP noted that although "the exact functioning of surveillance programmes around the world is not yet fully known ... it is *reasonably foreseeable* that the third country surveillance authorities *only* seem to obtain access to data after an international transfer from a company in the EU to another company outside the EU took place".[460] The fear of unauthorised access was also addressed thoroughly in 2016 (WP237) when the A29WP identified some "European Essential Guarantees" against "interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data".[461]

The attention placed by the EU legal framework on avoiding unauthorized access by foreign data protection authorities was also addressed in WP128. In this opinion, the A29WP found that the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a Belgian provider of financial messaging services had engaged in an unlawful transfer of personal data by mirroring data in the operation centres located in its US branches without, however, complying with the data transfer

---

[458] Article 29 Data Protection Working Party, *Working Document. Transfers of Personal Data to Third Countries. Applying Articles 25 and 26 of the EU Data Protection Directive (WP12)*, 1998, 21, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf.

[459] Article 29 Data Protection Working Party, *Opinion 7/2001 on the Draft Commission Decision (Version 31 August 2001) on Standard Contractual Clauses for the Transfer of Personal Data to Data Processors Established in Third Countries under Article 26(4) of Directive 95/46 (WP47)*, 2001, 3 (paragraph 2, italics mine), accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp47_en.pdf.

[460] Article 29 Data Protection Working Party, *Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes (WP228)*, 2014, 37 (italics mine), accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.

[461] Article 29 Data Protection Working Party, *Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection through Surveillance Measures When Transferring Personal Data (European Essential Guarantees) (WP237)*, 2016, accessed January 2, 2020, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

rules set out under the GDPR. The A29WP's decision was mainly driven by the fact that the transfer of data from the EU to the US had exposed personal data held by SWIFT to disclosure requests on the part of the US authorities: "by having decided to mirror all data processing activities in an operating centre in the US, SWIFT placed itself in a foreseeable situation where it is subject to subpoenas under US law".[462] In other words, by transferring data to its US operating centres, SWIFT found itself "exposed" to the US jurisdiction.[463] Following the transfer, the Belgian provider had, indeed, agreed to provide the United States Department of the Treasury with access to some message information stored in the US on the basis of subpoenas issued for terrorism investigation purposes. As it will be seen in chapter 5, the large-scale nature of access to data conducted by the US authorities is also at the basis of the invalidation of the Safe Harbour Agreement is *Schrems* and, more recently, of the request for a preliminary ruling raised by the Irish High Court with reference to Standard Contractual Clauses (*Schrems II*).[464]

4.3. Definition of Transfer

Definitional problems do not only affect the territorial scope of the Regulation, but also transfer mechanisms and, in particular, the very meaning of "transfer". No definition of transfer is provided under the 1995 Directive nor under the Regulation. The clarification which is given under both the 1995 Directive and the Regulation is that transfer of personal data (whatever that means) is relevant under EU data protection law when the data in question "are undergoing processing or are intended for processing after transfer".[465] As explained by the Information Commissioner's Office (ICO), the UK data protection authority, "[y]ou will be processing personal data in the UK and transferring it even if: you collect information relating to individuals on paper, which is not ordered

[462] Article 29 Data Protection Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128)*, 2006, 17, accessed January 2, 2020, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf.

[463] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 92.

[464] Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, Case C-311/18.

[465] Article 25(1) 1995 Directive and Article 44 GDPR.

or structured in any way; and you send this overseas with the intention that, once it is there, it will be processed using equipment operating automatically; or it will be added to a highly structured filing system relating to individuals".[466] This clarification has, however, a very limited relevance in narrowing down the processing activities which fall under the definition of "transfer". Indeed, the definition of "processing" that is given under Article 4(2) GDPR is so broad that almost every personal data that are "made available" in a non-EEA country are likely to undergo processing (e.g., simply storage of data in a third country).

An analysis of the concept of transfer, as it emerges from the OECD Guidelines and from Convention 108 will prove useful in composing the puzzle of the definition of "transfer". Paragraph 1 of the 1980 OECD Guidelines defines transborder flows of personal data as "movements of personal data across national borders".[467] Transfer is hence understood as the physical movement of data from the territory of one country to the territory of another country. This also emerges from paragraph 17 of the 1980 OECD Guidelines under which, as a general rule, Member countries "should refrain from restricting transborder flows of personal data between itself and *another member country* ".[468] The same definition of "transborder flows of personal data" is retained under the 2013 version of the Guidelines. Convention 108 seems to endorse the same understanding of the concept of transfer. Indeed, as seen above (4.2.1), Article 12 of Convention 108 provides that a Party shall not restrain the transborder flow of data "going *to the territory* of another Party", unless the "transfer is made *from its territory to the territory* of a non-Contracting State through the intermediary of the territory of another Party" when such transfer may lead to the circumvention of the law of the country of origin.[469]

[466] See ICO's archived guide to data protection: http://webarchive.nationalarchives.gov.uk/20180524151655/https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/.

[467] Paragraph 1(c), OECD Guidelines.

[468] Paragraph 17, OECD Guidelines (italics mine).

[469] Article 12(3)(b), Convention 108 (italics mine).

Interestingly, a different wording is adopted under Article 2 of the Additional Protocol to Convention 108. Under the said Article, "[e]ach Party shall provide for the transfer of personal data to a *recipient* that is *subject* to the *jurisdiction* of a State or organisation that is *not Party* to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer".[470] The Additional Protocol hence refers to the transfer of data to a *recipient* that is subject to a non-Party *jurisdiction* rather than to the *territory* of another country *per se*. This approach seems to be followed by the modernized version of Convention 108. Indeed, Article 14(2) of the Convention 108+ provides that "[w]hen the *recipient* is *subject* to the *jurisdiction* of a State or international organisation which is *not Party* to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured".[471] Recipient is then defined as "a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available".[472]

After having examined the concept of transfer, or at least what emerges of it, under the OECD Guidelines and Convention 108 (both in their "old" and revised versions), it is worth going back to the analysis of the 1995 Directive and the Regulation. Under both the DPD and the GDPR, transfer seems to be understood as the movement of data from an EEA country to a non-EEA country.[473] At the same time, the notion of transfer seems also to involve the presence of a data recipient who is subject to a third country's jurisdiction. The notion of "recipient" is also included and defined under both the 1995 Directive and the Regulation. Article 4(9) of the GDPR, which largely reproduces the definition of "recipient" under Article 2(g) of the DPD, defines "recipient" as "a natural or legal person, public authority, agency or another body, to which the personal data are *disclosed*, whether a third party or not",[474] while "third party" means "a natural or legal person, public authority, agency

[470] Article 2, Additional Protocol to the Convention 108 (italics mine).
[471] Article 14(2), Convention 108 + (italics mine).
[472] Article 2(e), Convention 108 +.
[473] Both Article 25 of the 1995 Directive and Article 44 GDPR, indeed, refer to the *transfer* of personal data to a third *country*.
[474] Article 4(9) GDPR (italics mine): "'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall

or body *other than* the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data".[475] With reference to the concept of "recipient" it is worth highlighting that although Article 44 GDPR perpetuates the wording "transfer of personal data ... to a third country",[476] unlike the 1995 Directive, the Regulation also uses the word "recipient" in the context of international transfer of data.[477] Recital 101 GDPR, for example, provides that "when personal data are transferred from the Union to controllers, processors or other *recipients* in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined" (italics mine); under Article 14(1)(f) GDPR, the controller shall inform the data subject of its intention to "transfer personal data to a *recipient* in a third country or international organisation" (italics mine); Article 15(1)(c) GDPR prescribes that the data subject shall be informed of "the *recipients* or categories of *recipient* to whom the personal data have been or will be disclosed, in particular *recipients* in third countries or international organisations" and "the categories of *recipients* to whom the personal data have been or will be disclosed including recipients in third countries or international organisations" should be included by the controller in its record of processing activities (Article 30(1)(d), italics mine).

Some other pieces of the puzzle can be added: several sources suggest that transfer of personal data entails the *communication* of such data to another recipient which will hence gain *access* to the data as a result of such transfer. Indeed, as seen above, Article 4(9) of the GDPR defines "recipient" as "a natural or legal person, public authority, agency or another body, to which the personal data are *disclosed*, ...".[478] The Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries also provides that a

not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing".

[475] Article 4(10) GDPR (italics mine).

[476] Article 44 GDPR.

[477] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 63.

[478] Article 4(9) GDPR (italics mine).

"disclosure of personal data to a data processor established outside the Community is an international transfer protected" under the 1995 Directive.[479]

The A29WP also seems to imply that transfer entails disclosure of (intelligible) data. Indeed, back in 1997, the A29WP noted that three types of transfer are possible under the 1995 Directive:

> 1) a communication of personal data by a data controller based in the Community to another data controller based in a third country;
> 2) a communication of personal data by a data controller based in the Community to a processor in a third country processing on behalf of the community-based controller;
> 3) a communication of personal data by a data subject based in the community to a data controller based in a third country.[480]

Likewise, a few years later, in WP74 (2003), the A29WP described transfer to third countries as "the *communication* of data to another data controller or data processor in a third country".[481]

Along the same lines, in the view of the LIBE Committee and of the EDPS, transfer means *communication* of personal data. Indeed, in its 2012 Draft report on the proposal for the GDPR, the LIBE Committee proposed to introduce a definition of transfer as "any *communication* of personal data, actively made available to a limited number of identified parties ...".[482] Similarly, in its opinion on the data protection reform package (2012), the EDPS noted that transfer "is aimed at *communicating* data to identified recipients...".[483] More explicitly, in its position paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies (2014), the EDPS stated that transfer would "normally imply the following elements: *communication,*

---

[479] Recital 10, European Commission, *Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC* (OJ L 6/52, 2001). This decision has been repealed by European Commission, *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 (2010/87/EU)* (OJ L 39/5, 2010).

[480] Article 29 Data Protection Working Party, *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy (WP4)*, 1997, 9, accessed January 2, 2020, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf.

[481] Article 29 Data Protection Working Party, *Working Document: Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (WP74)*, 2003, 8 (italics mine), accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf.

[482] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 65 (italics mine).

[483] European Data Protection Supervisor, *Opinion on the Data Protection Reform Package*, paragraph 109 (italics mine).

disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the [Regulation (EC) No 45/2001][484] *that the recipient(s) will have access to it*".[485]

Moving from the European to the national level, the German Data Protection Act defined transfer as the "the *revealing* to a third party of personal data which are stored or have been obtained by data processing in such a way that (a) the data are given to the third party or (b) the third party views or accesses data which is made available for view or access...".[486] Again, the use of the word "revealing" seem to entail access to data. The understanding of the concept of "transfer" as implying access to data can also be seen as implicit in the distinction between "accessibility" and "actual access" made by the ICO,[487] where only "actual access" involves transfer within the meaning of the EU data protection legislation (4.4.).

The understanding of the concept of "transfer" as entailing access to intelligible data justifies the uncertainties expressed, for example, by Rackspace, a cloud computing company which, back in 2009, in its response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data, noted that "it remains unclear whether using a storage device outside the EU, to store and process the data, constitutes a data transfer, where such

[484] European Parliament and Council of the European Union, *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data* (OJ L 8/1, 2000). This regulation has been repealed by European Parliament and Council of the European Union, *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* (OJ L 295/39, 2018).

[485] European Data Protection Supervisor, *Position Paper - The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies* (Brussels, 2014), 7, accessed December 15, 2019, https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf. "... The term would therefore cover both 'deliberate transfers' and 'permitted access' to data by recipient(s). The conditions of 'knowledge' and 'intention' would exclude cases of access through illegal actions (e.g. hacking). On the other hand, the mere fact that information might or will cross international borders to its destination due to the way in which networks are structured would not automatically trigger the concept".

[486] German Federal Data Protection Act, Section 3(8) (italics mine) quoted in Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 80.

[487] See ICO's archived guide to data protection: http://webarchive.nationalarchives.gov.uk/20180524151655/https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/.

data is *not accessed* or *manipulated* in this country".[488] However, as a "response" to the uncertainties expressed by Rackspace, it should be noted that even the storage of encrypted data in a cloud service provider that is located outside the EEA, and hence the storage of data to which the cloud service provider has *no* access since data are encrypted amounts to "transfer" under to scope of the GDPR. This derives from the combination, on the one hand, of the broad definition of the concept of "processing" (which includes data storage) and, on the other hand, of the fact that encrypted data are still personal data under the GDPR. Indeed, as noted by the A29WP in 2012, "[i]n a cloud environment, encryption may significantly contribute to the confidentiality of personal data if implemented correctly, although it does not render personal data irreversibly anonymous".[489]

As a final consideration, it should be noted that data transfer rules do not apply when data are transferred directly from a data subject in the EU to a non-EEA data controller or processor nor when data are transferred from an EEA data controller/processor to a non-EEA data subject. In other words, data transfer rules only apply to data transfers from an EEA data controller/processor to a non-EEA data controller/processor. For example, if an hotel in the UK takes bookings from customers across the globe, including from customers outside the EU and then sends the data back to those individuals, including their name and email address, such transfer from the hotel to its customers would not be not restricted under the GDPR. On the other hand, if the hotel in Germany makes use of a cloud service provider for storing and managing the data of its customers and the said cloud service provider has several data centres across the globe, the German hotel should make sure that data are transferred outside the EEA compliantly with the EU data transfer rules.[490] At the same time, it should be noted that when a non-EEA organisation processes the data of data subjects in the EU and, by virtue of that processing, data are transferred from the data subject in the EU to the non-EEA organisation in

[488] Rackspace, *Consultation Paper on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009, 5 (italics mine), accessed July 31, 2018, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/unregistered_organisations/rackspace_us_inc_en.pdf.

[489] Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing (WP196)*, 2012, 15 (paragraph 3.4.3.3), accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[490] See the ICO's guide on international data transfer in case of no-deal Brexit: https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-theres-no-brexit-deal/the-gdpr/international-data-transfers/.

question, the said non-EEA organization is likely to be caught under the territorial scope of the GDPR. In other words, when data are transferred from data subjects in the EU to non-EU data controllers/processors, the provisions on data transfer do not apply but the whole scope of the GDPR is likely to apply by virtue of Article 3 GDPR (for example, if the non-EEA data organization is offering goods or services to the data subjects or is monitoring their behaviour).

4.4. Transfer in Web Hosting: *Bodil Lindqvist*

The Internet allows data to become accessible by anyone who visits the website in any part of the world. When using webhosting providers, data are first uploaded to the provider's servers (where data are stored) and then downloaded by those who visit the website. The webhosting provider can either be established in the EEA or outside the EEA. In both cases, the provider can use infrastructures located in the EEA or in a third country or in both the EEA and in a third country. The emergence of similar scenarios was clearly not envisaged by the EU co-legislators when drafting the 1995 Directive.[491] In *Bodil Lindqvist*,[492] the ECJ dealt with the difficulties of applying the DPD, where no provisions concerning the use of the Internet have been included, to such new scenarios. Precisely, the ECJ was required to establish whether the upload of personal data by an individual in the EU onto an Internet page (with the result that personal data become accessible worldwide) which is hosted by an EU-established hosting provider constitutes a transfer of data within the meaning of the 1995 Directive. This question was raised in criminal proceedings before a Swedish Court against Mrs Lindqvist, a church volunteer, who was charged of having breached the Swedish data protection law for having uploaded on a webpage information about her parishioners without having obtained their consent nor notified the Swedish data protection authority.

The observations submitted to the ECJ witness the complexities of this scenario. The European Commission and the Swedish Government took the view that the loading of personal data

[491] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 76–78.

[492] Judgment of the Court of 6 November 2003, *Bodil Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

onto an Internet page constitutes transfer of data within the meaning of the 1995 Directive since the result of that activity is that personal data become accessible to third countries' nationals. The same conclusion applies if no one has access to the data from outside the EEA and if the server is located in a third country.[493] The Dutch Government reached the opposite conclusion in stating that the term transfer "must be understood to refer to the act of *intentionally* transferring personal data from the territory of a Member State to a third country and, second, that no distinction can be made between the different ways in which data are made accessible to third parties".[494] On the other hand, the UK government submitted that "Article 25 of Directive 95/46 concerns the transfer of data to third countries and not their accessibility from third countries. The term 'transfer' connotes the transmission of personal data from one place and person to another place and person".[495] It is only in this event that States are required to comply with the data transfer rules set out in the 1995 Directive.[496]

The ECJ started its reasoning from some technical considerations. It noted that in order for a web page to be published on the Internet, the data making up that page have to be transmitted to the hosting provider. The provider manages the infrastructures needed to store those data and to connect the server to the Internet. The provider's infrastructures can be located in one or more countries other than the country where the hosting provider is established.[497] The ECJ then highlighted the distinction between the uploading and downloading of data when it stated that "Mrs Lindqvist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages". Indeed, in order to obtain the information *uploaded* by Mrs Lindqvist, an Internet user would need not only to connect to the Internet but also to take the actions to consult, and hence *download*, that information.[498] It follows that "personal data which appear on

[493] Ibid., paragraph 53.
[494] Ibid., paragraph 54 (italics mine).
[495] Ibid., paragraph 55.
[496] Ibid.
[497] Ibid., paragraph 59.
[498] Ibid., paragraph 60.

the computer of a person in a third country, coming from a person who has loaded them onto an internet site, were not directly transferred between those two people but through the computer infrastructure of the hosting provider where the page is stored".[499]

It is in this context that the ECJ examined whether the concept of transfer also includes the uploading of data carried out by Mrs Lindqvist and reached the following conclusion:

> Given, first, the state of development of the internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.[500]

Indeed, interpreting the concept of transfer of data to third countries as also including the uploading of personal data onto an Internet page entails that there would be transfer of data within the meaning of Article 25 of the 1995 Directive to *all* the non-EEA countries where there are the technical means for accessing the Internet. This interpretation would transform the *special* regime provided by the Directive in the event of data transfer in "a regime of *general* application, as regards operations on the internet".[501] As a result, "if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent *any* personal data being placed on the internet".[502] Accordingly,

> there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is *established* in *that State* or in *another Member State*, thereby making those data accessible to anyone who connects to the internet, including people in a third country.[503]

Given this conclusion, the ECJ deemed unnecessary to investigate whether an individual outside the EEA had accessed the data or whether the server of the hosting provider was located in a third

[499] Ibid., paragraph 61.
[500] Ibid., paragraph 68.
[501] Ibid., paragraph 69 (italics mine).
[502] Ibid.
[503] Ibid., paragraph 71 (italics mine).

country.[504] The Court ruling was hence limited to the analysis of the *uploading* activities carried out by an individual in the EEA (i.e., the uploader) to an *EEA-established* hosting provider.

Given the narrow focus of the ruling, several questions remain unanswered. Firstly, once data have been uploaded to an EEA-established provider (as it was the case in *Bodil Lindqvist*), does transfer occur upon the *downloading* of such data by an Internet user located in a third country? The negative answer seems to be supported by the ECJ's statement that the uploading of data does not constitute transfer regardless of whether individuals in third countries have access to those data.[505] However, a conflation of the two concepts (uploading and downloading) seems to go against the explicit decision of the ECJ to confine its judgement to the uploading of data with the exclusion of other (possible) subsequent actions.[506] Moreover, concluding that the download of data *never* entails transfer would translate into a "loophole for companies to escape the application of the EU data transfer restrictions by hosting global databases on a server in the EU and making them accessible via the Internet".[507]

One view could be that the download of data constitutes transfer within the meaning of Article 25 of the 1995 Directive only when such download involves the transmission of data to some *specific* recipients rather than to an indiscriminate number of individuals. The EDPS seems to have endorsed this view when, in 2007, in interpreting Article 9 of Regulation (EC) No 45/2001[508] in the light of *Bodil Lindqvist*, it noted that "[t]he emphasis in the Court's analysis on a *publicly* accessible website implies that its conclusions do not seem to apply to situations where the Internet is used as a technical platform for *closed* groups of users". Consistently, while "the *world wide publication* of personal data on the Internet, through a public website" should not be counted as transfer under Article 9 of Regulation (EC) No 45/2001, transfer would occur in cases involving "a *closed* website or an intranet

[504] Ibid., paragraph 70.
[505] Ibid.
[506] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 82.
[507] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 156.
[508] Article 9 of Regulation (EC) No 45/2001 sets out rules on the "[t]ransfer of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC".

which is only accessible for a *defined* group of users". In similar situations, in fact, problems of transforming the special regime detailed in Chapter IV of the Directive in a "regime of general application" would not arise[509] since closed websites or intranets do not involve an indefinite number of countries but specific end-users.[510] The European Union Agency for Fundamental Rights (FRA) and the Council of Europe (2014) seem to follow the same approach when they stated that "[t]he principle that mere publication of (personal) data is not to be considered as transborder data flow applies also to online public registers or to mass media, such as (electronic) newspapers and television. Only communication which is *directed* at *specific recipients* is eligible for the concept of 'transborder data flow'".[511]

A seemingly opposite approach was proposed by Kuner (2007) when he suggested that "making personal data available on the internet can be viewed as a kind of data transfer if it involves granting access to the data of other parties ... on a large scale and for business purposes".[512] Kuner reached this conclusion by highlighting the several, peculiar factors on the basis of which the ECJ delivered its ruling in *Bodil Lindqvist*, such as the absence of evidence that personal data were actually accessed by individuals outside the EEA, the fact that the information has been published in Swedish and was meant to be accessed by a small number of people (i.e., the members of a church community) and that the ECJ may have sympathized with Mrs Lindqvist. In Kuner's view, all these circumstances might limit the relevance of the ECJ's judgment to the specific facts of the case: "a company placing a large amount of data on the internet and making it available to large numbers of employees, customers, or contractors on a pan-European or global scale would probably be viewed by the DPAs as engaging in an activity so different in scale from that at issue in *Lindqvist* as to bring it within the

[509] European Data Protection Supervisor, *Replies to a Request for Cooperation or Consultation under Articles 24(b) Respectively 46(d) of Regulation (EC) 45/2001 Concerning the Publication of Personal Data on the Internet and the Applicability or Not of Article 9 of the Regulation* (Brussels, 2007), 3 (italics mine), accessed May 13, 2018, https://edps.europa.eu/sites/edp/files/publication/07-02-13_commission_personaldata_internet_en.pdf.

[510] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 83.

[511] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Luxembourg, 2014), 131 (italics mine), accessed November 30, 2019, https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

[512] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 156.

definition of 'data transfer'".[513] However, despite Kuner's emphasis on the *large scale* of activities with which most of the companies engage when they make a *large* amount of data available to a *large* number of people, his interpretation does not seem to differ substantially from the one suggested by the EDPS (2007), and by the FRA and the Council of Europe (2014). Indeed, from the examples of transfer of data through the Internet that he proposes, it is clear that Kuner is also referring to cases where transfer of data is directed at *specific* users (no matter how many they are), such as in the case where a company "puts its employee or customer database on the internet for the purpose of worldwide access by its *human resource staff*, *salespeople*, etc".[514]

The ICO adopted a different approach in examining the ruling in *Bodil Lindqvist*. Precisely, in interpreting the ECJ's findings in this case, the UK data protection authority drew a line between the mere accessibility of the (uploaded) data by persons in third countries and the actual access of data by those persons. The intention behind the transfer is equally relevant in ICO's view:

> Putting personal data on a website will often result in transfers to countries outside the EEA. The transfers will take place when someone outside the EEA *accesses* the website. If you load information onto a server based in the UK so that it can be accessed through a website, you should consider the likelihood that a transfer may take place and whether that would be fair for the individuals concerned. If you *intend* information on the website *to be accessed* outside the EEA, then this is a transfer.[515]

On this basis, if a controller uploads data to an EEA-established web-hosting provider and intends those data to be accessed by individuals outside the EEA, a transfer (within the meaning of the DPD and the GDPR) would take place upon the actual access by those individuals. Conversely, transfer would not occur when information published online is accessed by people outside the EEA, but the controller did not intend this access to occur. As seen above, a similar interpretation was also suggested by the Dutch government in its submission to the ECJ in *Bodil Lindqvist* when it interpreted the concept of transfer as "the act of *intentionally* transferring personal data from the territory of a

[513] Ibid., 83.
[514] Ibid. (italics mine).
[515] See ICO's archived guide to data protection: http://webarchive.nationalarchives.gov.uk/20180524151655/https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/.

Member State to a third country".[516] Consistently, in 2007, the Dutch DPA reiterated that "[o]nly those controllers who *explicitly intend* to transfer data to a country outside of the EU, as may be the case in a multinational company that operates an *intranet* comprising personal data, must comply with the regulations relating to transfer".[517]

A similar approach was adopted by the EDPS in 2012 in his opinion on the data protection reform package. In its opinion, after having recalled that according to the ECJ a publication on the Internet does not represent *per se* a data transfer within the scope of the 1995 Directive, the EDPS noted that, in order to determine whether transfer has occurred or not, it should be taken into account, among others, "whether the data has been made freely available with the *aim* of *giving access* to it *and* whether the transfer is likely to have *actually reached* one or more *recipients* abroad".[518] In its 2012 opinion, the EDPS seems hence to follow the distinction between mere accessibility of data and actual access of data. Equally, according to the EDPS, transfer should also be supported by the sender's *intention* of making such data accessible to the recipient when it stated that it should be determined whether the data has been made available "with the aim of giving access to it". Interestingly, the LIBE Committee deemed a definition of transfer necessary within the GDPR in order to "distinguish [transfer] from making data (publicly) available". To this aim, as seen above (4.3.), in its 2012 Draft report on the proposal for the GDPR, the LIBE Committee proposed to introduce the following definition: "'transfer' means any communication of personal data, *actively* made available to a *limited* number of identified parties, with the *knowledge* or *intention* of the sender to give the recipient access to the personal data".[519] Following this definition, and consistently with the opinions cited above, according to the LIBE Committee, transfer within the scope of the GDPR

[516] *Bodil Lindqvist*, paragraph 54 (italics mine).

[517] Dutch DPA, *Publication of Personal Data on the Internet*, 2007, 49 (italics mine), accessed May 14, 2018, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_20071108_richtsnoeren_internet.pdf.

[518] European Data Protection Supervisor, *Opinion on the Data Protection Reform Package*, paragraph 109 (italics mine).

[519] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 65 (italics mine).

differs from mere publication of data since it is directed at specific and identified parties. Moreover, as a further condition for the applicability of the data transfer provisions, such transfer should also be supported by the intention (or the knowledge) of the sender to give the recipient access to those data.

In the light of the opinions and proposed definitions examined above, it can be argued that the download of data constitutes transfer within the scope of the EU data protection legislation only to the extent that it involves the transmission of data to some specific individuals. This view seems to be consistent with the anti-circumvention objective underpinning data transfer rules. Indeed, as recalled by the EDPS in his 2012 opinion on the data protection reform package, the reason why when determining whether a transfer has occurred it should be taken into account "[t]he fact that it is aimed at communicating data to *identified recipients*" is that this is the only interpretation that "justifies the assessment of the level of protection guaranteed by the (*country* of the) *recipient*, as well as possible measures to be taken in order to ensure the protection of the data".[520] In other words, transfer within the scope of the EU data protection legislation should be understood as transfer of data directed at some *identified* recipients since this interpretation justifies the need to assess the level of data protection guaranteed by the jurisdiction to which the recipient is subject as prescribed by Article 25 DPD and Article 45 GDPR.

Another question remains open with reference to the position of the web-hosting provider: is there a transfer by the uploader if the provider is *not* established in the EEA? This question arises from the emphasis placed by the ECJ on the fact that the hosting provider was established in the EEA. Since the web-hosting provider can be considered as a "recipient" to which the data uploaded to its service are transferred and considering that the "uploader" acts as a data controller which is subject to the GDPR requirements, including the requirements concerning data transfer, it seems reasonable to conclude that the uploading of data would constitute a transfer if the provider is established outside the EEA. The transfer would hence take place from the EEA data controller (in this case, the uploader)

[520] European Data Protection Supervisor, *Opinion on the Data Protection Reform Package*, paragraph 109 (italics mine).

to the web hosting provider (i.e., the non-EE data recipient) but *not* from the EEA data controller to the rest of the world.

4.5. Transfer or Transit?

Neither the 1995 Directive nor the GDPR explicitly exclude transit of personal data through third countries from the application of data export restrictions prescribed under Chapter IV and V respectively. The DPD, however, excluded mere transit of data through the EU as a possible trigger for the applicability of the EU jurisdiction under Article 4(1)(c). As seen above (3.4.2.), in fact, Article 4(1)(c) prescribes the applicability of the EU jurisdiction in the event that a non-EEA controller "makes use of equipment, ..., situated on the territory of the said Member State, *unless* such *equipment* is used only for purposes of *transit through* the *territory* of the *Community*" (italics mine). Again, no definition of "transit" has been provided by the EU co-legislators. A definition can, however, be found in the Explanatory Memorandum of the OECD Guidelines, where data in transit are defined as "data which pass through a Member country without being used or stored with a view to usage in that country".[521]

Some indications about the meaning of transit can also be found in WP179 where, in commenting on Article 4(1)(c) of the 1995 Directive, the A29WP described transit "as for example … the case of telecommunication networks (cables) or postal services which only ensure that communications transit through the Union in order to reach third countries".[522] Since transit was irrelevant in determining the territorial scope of the DPD, it can be argued that transit should be equally excluded from the applicability of data export restrictions. This view has been shared by many commentators. Among others, Blume (2000) noted that rules on data transfer to third countries "concern transfer and not transmission: for example in the case of telecommunication networks

[521] Paragraph 66, *Explanatory Memorandum*, 1980 OECD Guidelines.
[522] Article 29 Data Protection Working Party, *WP179*, 30.

(cables) or postal services which only ensure that communications transit through the Union in order to reach third countries".[523] Similarly, Kuner (2007) argued that:

> The mere fact that personal data are transferred via the internet from one EU Member State to another, which may mean that they are routed across the borders of a non-EU country because of the architecture of the internet, does not result in the application of the General Directive's restrictions on international transfers, as long as the presence of the data in the non-EU country is limited to mere transit and no further processing is performed on it there.[524]

The ICO also explicitly excludes transit from the application of data export restrictions. For example, in the case where "[p]ersonal data is transferred from country 'A' to country 'B' via a server in country 'C', which does not access or manipulate the information while it is in country 'C'", transfer would only be to country B.[525] As a further example, if data are transferred from a data controller in France to a data controller in Ireland through a server in Australia and "[t]here is no intention that the personal data will be accessed or manipulated while it is in Australia", the transfer will only be to Ireland.[526]

In the light of the above, data export restrictions should not apply when data are merely "passing through" non-EEA countries. This interpretation does not seem to be incompatible with the anti-circumvention purpose underpinning data export restrictions. Data in transit merely pass through a country without being "used or stored" and hence without being processed. A misuse of those data in the country through which data transit should not be a risk since data are not meant to be used at all. At the same time, however, appropriate protection, especially in technical terms (e.g., by encrypting data), should be guaranteed even when data are in transit since the transit of data through "insecure" countries may increase data exposure to foreign authorities (and in particular to intelligence agencies' wiretapping).

---

[523] Peter Blume, "Transborder Data Flow: Is There a Solution in Sight?," *International Journal of Law and Information Technology* 8, no. 1 (January 1, 2000): 82–83.

[524] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 156.

[525] See ICO's archived guide to data protection: http://webarchive.nationalarchives.gov.uk/20180524151655/https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/.

[526] See the ICO's guide on international data transfer: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers#admin

This increased "exposure" to foreign authorities when data are in transit, and consequently the need to protect data from this exposure, was explicitly recognized in WP238[527] and WP255[528] where the A29WP clarified that "the Privacy Shield Principles will apply from the moment the data transfer takes place"[529] including when data is "on its way" to the country of destination.[530] Equally, the EDPS, in its 2016 Opinion on the EU-U.S. Privacy Shield draft adequacy decision, stressed the risk of "potential collection once [data are] transferred and notably when in transit".[531] However, this exposure is unlikely to be solved by in-country data storage and routing. Foreign public authorities may, in fact, still gain access to data in several ways: by means of remote access; by means of cooperation with other foreign public authorities (2.4); by requesting direct cooperation to the companies holding those data (5.8.2.).

4.6. Conclusion

This chapter has shown that the primary purpose of data transfer rules is to ensure that the high standards of data protection guaranteed by the EU legislation are not circumvented once data are transferred outside the EU borders. International data transfer is hence subject to some strict requirements which aim to ensure that individuals continue to benefit from the rights and freedoms they are granted in the EU, regardless of data location. The analysis conducted above has, however, shown that another policy objective seems to underpin data transfer rules, i.e., protecting data from unauthorized access or disclosure requests by foreign public authorities. Indeed, when data are transferred to third countries, such data may be exposed to public interventions that infringe upon the essence of fundamental rights and freedom and that go beyond what is necessary in a democratic society. The SWIFT case is illustrative in this respect since the A29WP concluded that, by having

[527] Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision (WP238)*, 2016, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[528] Article 29 Data Protection Working Party, *EU – U.S. Privacy Shield – First Annual Joint Review (WP255)*, 2017.

[529] Article 29 Data Protection Working Party, *WP238*, 12.

[530] Article 29 Data Protection Working Party, *WP255*, 16.

[531] European Data Protection Supervisor, *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, 2016, 6–7.

decided to mirror (and hence) transfer data to its US data centres, the Belgian provider had exposed itself to a situation where it is subject to disclosure requests by US authorities.

In the absence of an official definition of the notion of "transfer", the second part of the chapter aimed to bring together some pieces of the puzzle that compose the concept of "transfer". The analysis has shown that transfer is generally understood as the movement of data from the territory of one country to the territory of another country. Transfer of data seems also to (generally) involve the presence in the third country in question of a recipient that is (generally) subject to the jurisdiction of the said third country. Moreover, several sources suggest that the transfer of data entails the *communication* of such data to the recipient which will hence gain *access* to the data as a result of the transfer. The concepts of "transfer" of data and "disclosure" of such data seem in fact to overlap in several definitions that have been examined. At the same time, it has been argued that the conflation of these two concepts does not seem to be completely accurate since, for example, even the transfer of encrypted data to a non-EEA service provider for storage purposes would fall within the scope of the data transfer provisions set out under the GDPR.

A line can also be drawn between "transfer" and "making data publicly available". Indeed, in *Bodil Lindqvist*, the ECJ concluded that there is no transfer within the meaning of the GDPR when data are loaded online thus making them potentially available all over the world. At the same time, while the world-wide publication of personal data online does *not* amount *per se* to a transfer within the scope of the GDPR, a transfer would take place if data are made available to some *specific recipients* and hence to a limited number of identified people. The distinction between access and mere accessibility seems also to be relevant in establishing whether the uploading of personal data on a website amounts to transborder data flow. The ICO, indeed, suggests that transfer of data takes place upon *actual access* to the uploaded data by individuals outside the EEA and not upon the mere accessibility of such data. As a further element, the sender's *intention* to transfer data seem also to be relevant: it has been suggested by several parties (i.e., the ICO, the Dutch DPA and the EDPS) that only data controllers which explicitly *intend* to transfer data outside the EEA are required to comply

with data transfer provisions. Lastly, it can be reasonably concluded that data transfer provisions do not apply to the *transit* of data through *third* countries. In other words, the mere fact that data pass through a non-EEA country without being processed in any way should not be a trigger for the applicability of data transfer rules. Keeping these concepts in mind, and in particular the two objectives underpinning the provisions on data transfer, the next chapter will investigate the content of such provisions.

5. Restrictions on International Data Transfer: Untangling Data Transfer Mechanisms

5.1. Introduction

The EU data protection framework does not ban the transfer of data outside the EU, but it makes transfer to non-EEA countries conditional upon compliance with some specific rules. Indeed, under Chapter IV of the 1995 Directive and Chapter V of the GDPR, transfers of data to third countries are subject to what have been defined as "cumbersome", "unnecessarily expensive", and "time-consuming" mechanisms.[532] In its 2017 communication to the European Parliament and the Council, the European Commission argued that the GDPR provides for a "renewed and diversified toolkit for international transfers".[533] However, even though the GDPR has introduced some simplifications together with some new legal bases for transfers, the architecture of transfer mechanisms remains essentially the same. This chapter will analyse the grounds on which data can be transferred to third countries; what has changed and what has not in comparison to the provisions under the 1995 Directive; the strengths and the weaknesses of data transfer provisions in both enabling data flow and in protecting data not only from unlawful processing but also from unauthorised access by foreign public authorities.

5.2. From the 1995 Directive to the GDPR: Comparing and Contrasting Transfer Mechanisms

No substantial changes have been introduced under the GDPR with reference to the transfer of personal data to third countries. The GDPR expands and formalizes the use of existing legal bases for international data transfer; it provides for some simplifications by abolishing the general requirement of prior authorization by national data protection authorities;[534] it includes the possibility to provide for appropriate safeguards by means of approved codes of conduct and certification

[532] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 152.

[533] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 4.

[534] Article 46(2) GDPR.

mechanisms,[535] and by means of legally binding instruments or administrative arrangements between public authorities or bodies;[536] it contains a new derogation based on "compelling legitimate interests pursued by the controller",[537] and empowers the European Commission to develop international cooperation mechanisms and to provide international mutual assistance to facilitate the enforcement of data protection legislation.[538] Data transfer provisions are also explicitly extended to onward transfers and to transfers to international organizations. In addition, data transfer provisions shall be complied with not only by the controller but also by the processor.[539] The table below aims to compare and contrast data transfer provisions under the DPD and those under the GDPR:

Chapter IV DPD	Chapter V GDPR
Art.25: Transfer on the basis of an **adequacy decision** **Art.26:** In the absence of an adequacy decision, some **derogations** apply: • Consent of the data subject • Performance or conclusion of a contract or implementation of pre-contractual measures • Public interest • Establishment, exercise or defence of legal claims • Vital interest of the data subject • Transfer from a register (Art.26(1)) • **Adequate safeguards** adduced by the *controller* **with the authorization** of a Member State, in particular appropriate contractual clauses (Art.26(2)): - Standard contractual clauses approved by the European Commission (Art.26(4)) - Ad hoc contracts - Binding corporate rules[540]	**Art.45:** Transfer on the basis of an **adequacy decision** **Art.46:** In the absence of an adequacy decision, transfer can take place if the *controller* or the *processor* provides **appropriate safeguards**:[541] • Appropriate safeguards **without** specific **authorization** from a supervisory authority: - Legally binding instrument between public authorities or bodies [NEW] - Binding corporate rules (Article 47) - Standard contractual clauses adopted by the European Commission - Standard contractual clauses adopted by a supervisory authority and approved by the European Commission [NEW] - Code of conduct pursuant to Art.40 [NEW] - Certification mechanism pursuant to Art.42 [NEW] • Appropriate safeguards **with authorization** from a supervisory authority: - Contractual clauses between controller/processor and controller/processor/recipient (e.g., ad hoc contracts)

[535] Article 46(2)(e) and Article 46(2)(f) GDPR.

[536] Article 46(2)(a) and Article 46(3)(b) GDPR.

[537] Article 49(1) paragraph 2 GDPR.

[538] Article 50 GDPR.

[539] "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to *an international organisation* shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller *and processor*, *including for onward transfers* of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined". Article 44 GDPR (italics mine).

[540] Binding corporate rules were not explicitly envisaged by the 1995 Directive but they were developed by the A29WP on the basis of an extensive interpretation of Article 26(2) DPD (see 5.5.2).

[541] The GDPR has renamed "adequate safeguards" (Article 26(2) DPD) to "appropriate safeguards" (Article 46 GDPR).

	- Provisions in administrative arrangements between public authorities or bodies [NEW] **Art.48:** Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable if based on an **international agreement** (e.g., MLATs) **Art.49(1):** In the absence of an adequacy decision or of appropriate safeguards, some **derogations** apply: • Consent of the data subject • Performance or conclusion of a contract or implementation of pre-contractual measures • Public interest • Establishment, exercise or defence of legal claims • Vital interest of the data subject or other persons [partially NEW][542] • Transfer from a register **Art.49(1) paragraph 2:** In the absence of an adequacy decision or of appropriate safeguards, and of derogations for specific situations, a transfer may take place if it is necessary for the purposes of compelling **legitimate interests** pursued by the controller [NEW]

Table 5 – Comparison Chapter IV DPD – Chapter V GDPR

The GDPR lays out a clear hierarchy between transfer mechanisms. As a general rule, transfer of personal data may take place only when a third country or an international organization "ensures an adequate level of data protection" (Article 45 GDPR); in the absence of an adequacy decision pursuant to Article 45 GDPR, transfer may take place only if "the controller or processor has provided appropriate safeguards" (Article 46); in the absence of an adequacy decision pursuant to Article 45 GDPR and of appropriate safeguards pursuant to Article 46 GDPR, transfer may take place following the derogations for specific situations laid out in the first paragraph of Article 49 GDPR; in the absence of an adequacy decision pursuant to Article 45 GDPR, of appropriate safeguards pursuant to Article 46 GDPR and of the derogations for specific situations pursuant to Article 49(1) paragraph 1, a transfer may take place for a compelling legitimate interest pursued by the controller pursuant to Article 49(1) paragraph 2 GDPR.

[542] This derogation has been extended so as to include vital interests not only of the data subjects but also of third parties (5.6.).

A similar hierarchy was also established under the 1995 Directive, but it was not clearly reflected in its wording. The relationship between the different legal bases for transfer of data was however clarified by the A29WP in 2005 (WP114). First and foremost, transfer could take place if the third country in question ensured an adequate level of protection (Article 25 DPD). Secondly, and by way of derogation from Article 25 DPD, transfer could take place if the controller "adduces adequate safeguards" (Article 26(2) DPD). As a last resort, transfer could be framed on the basis of one of the derogations set out under Article 26(1) DPD.[543]

Interestingly, the hierarchy set out under the GDPR does not always match the order of "preference" laid out by some cloud providers in their DP Agreements. For example, Salesforce provides that, in the event that its services are covered by more than one data transfer mechanisms, the following order of precedence should be observed: 1) Binding Corporate Rules (BCRs), 2) EU-US and Swiss-US Privacy Shield Framework self-certifications, and 3) Standard Contractual Clauses (SCCs).[544] Similarly, Box's DP Agreement provides that BCRs shall take precedence over the EU-US and Swiss-US Privacy Shield Framework self-certifications.[545] Both Salesforce and Box have hence placed BCRs on top of an adequacy decision, i.e., the EU-US Privacy Shield (5.4.4), thus patently subverting the hierarchy set out under the GDPR (and by the 1995 Directive before it). It is possible that national data protection authorities may consider this "subverted" hierarchy not compliant with the GDPR.[546]

[543] Article 29 Data Protection Working Party, *WP114*, 4–5.

[544] Section 11.4, Salesforce, Data Processing Addendum (Revision November 2018), accessed April 25, 2019, https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf.

[545] Section XIV.B, Box, Data Processing Addendum. Box's Data Processing Addendum is not publicly available but instructions on how to sign a DP Agreement are available on Box's website ("Sign your DPA"): https://www.box.com/en-gb/gdpr.

[546] Dimitra Kamarinou, Christopher Millard, and Isabella Oldani, *Compliance as a Service* (Queen Mary School of Law Legal Studies Research Paper No. 287/2018, 2018), 27, accessed April 25, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3284497.

5.3. The Transfer of Data to the United Kingdom after Brexit

The United Kingdom withdrew from the European Union on 31 January 2020. Pursuant to Articles 126 and 127 of the Withdrawal Agreement[547] that have been ratified by the European Union and the UK, there will be a transition period until 31 December 2020 during which EU law, including the GDPR, will continue to apply to the UK. This entails that the transfer of data from the EU to the UK will remain untouched until the end of year and no data transfer mechanism will need to be implemented to EU-UK transfers. As of 1 January 2021, EU law will cease to apply to the UK and the aforementioned data transfer mechanisms will also need to be implemented in order to allow the lawful transfer of data from the European Union to the United Kingdom. The default position at the end of the transition period will hence be the same as in the event of a non-deal Brexit.[548]

A number of notices have already been published over the past two years by the EU institutions in order to prepare stakeholders in the event of a no-deal Brexit. In January 2018, the European Commission released a notice to stakeholders on the withdrawal of the United Kingdom in which it clarified that the EU data protection rules will cease to apply to the UK from the exit date. This entails that, unless provided otherwise in the Withdrawal Agreement, data transfer rules will apply to the transfer of data to the United Kingdom.[549] As for the use of personal data that have been obtained by UK-based controllers/processors *before* the withdrawal date, the European Commission clarified that the processing of such data by UK entities can continue as long as the principles of the EU data protection law are implemented. Otherwise, such data should be deleted or destroyed.[550]

---

[547] *Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (2019/C 384 I/01)* (OJ C 384 I/1, 2019).

[548] Information Commissioner's Office, "Information Rights and Brexit Frequently Asked Questions," accessed June 25, 2020, https://ico.org.uk/for-organisations/data-protection-and-brexit/information-rights-and-brexit-frequently-asked-questions/.

[549] European Commission, *Notice to Stakeholders. Withdrawal of the United Kingdom from the Union and EU Rules in the Field of Data Protection*, 2018, accessed December 8, 2019, https://ec.europa.eu/info/sites/info/files/file_import/data_protection_en.pdf.

[550] European Commission, *Position Paper on the Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date*, 2017, accessed December 8, 2019, https://ec.europa.eu/commission/sites/beta-political/files/data_and_protection.pdf.

A similar information note on data transfers to the UK in the event of a no-deal Brexit was released a year later, on 12 February 2019, by the EDPB. The EDPB has identified five steps that should be taken by the organizations when transferring data to the UK: (1) identify the processing activities that entail a transfer of data to the UK; (2) identify the data transfer mechanism under which data transfer will be framed; (3) implement the chosen data transfer mechanism before the exit date; (4) include in the internal documentation of the organization reference to the fact that data will be transferred to the UK; (5) update accordingly the privacy notice laid out by the organization.[551] In July 2019, the EDPS has also released an information note on international data transfer after Brexit building on the guidance provided by the European Commission and the EDPB.[552] Again, the EDPS recalled that in a no-deal Brexit scenario, the EU data protection law would no longer apply to the UK. This would have an immediate repercussion on the data flow from the EU institutions to the UK. The EDPS hence suggested that the EU institutions take the following steps in order to be prepared for a no-deal scenario: the EU institutions should map the processing activities they conduct, they should review and implement the available data transfer mechanisms before the exit date, and update accordingly the internal documentation and data protection notice.[553]

In the meantime, the UK Government has clarified that the transfer of data from the United Kingdom to the European Union will not be restricted so that UK organisations will still be able to lawfully transfer data to the European Union.[554] At the same time, in the Political Declaration setting out a framework for the future relationship between the European Union and the United Kingdom as agreed on 17 October 2019, the European Commission committed to begin its adequacy assessment of the data protection standards offered by the UK pursuant to Article 45 GDPR, endeavouring to

[551] European Data Protection Board, *Information Note on Data Transfers under the GDPR in the Event of a No-Deal Brexit*, 2019, accessed December 8, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexit_en.pdf.

[552] European Data Protection Supervisor, *Information Note on International Data Transfers after Brexit*, 2019, accessed December 8, 2019, https://edps.europa.eu/sites/edp/files/publication/19-07-16_for_translation_note_on_personal_data_transfers_post-brexit_en.pdf.

[553] Ibid., 5–6.

[554] Information Commissioner's Office, "Information Rights and Brexit Frequently Asked Questions."

adopt a decision by the end of 2020 if the conditions for such a decision are met.[555] The steps that companies will need to take in order to continue the transfer of data after 31 December 2020 is hence very much dependant on whether the EU Commission will adopt an adequacy decision by the end of the transition period. It should also be recalled that many UK companies doing business in the EU are likely to fall under the territorial scope of the GDPR pursuant to Article 3 GDPR, meaning that they will continue to be directly subject to the GDPR.

5.4. Adequacy Decisions

5.4.1. From Article 25 of the 1995 Directive to Article 45 of the GDPR

Article 45 GDPR follows the tradition established under Article 25 of the 1995 Directive in prescribing that "[a] transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection".[556] Compared to Article 25 DPD, Article 45 GDPR has expanded the powers of the European Commission by allowing the European Commission to assess the adequacy not only of a third country but also of a territory or of a specific sector within that country or of an international organization. This change should be welcomed since in many countries, different sectors are covered by different laws so that even if the level of protection afforded by a third country's legal system is not "adequate" as a whole, some specific sectors may still be found adequate.[557]

Article 45 then specifies the elements that the European Commission shall take into account when assessing the adequacy of the level of protection, such as, among others, the rule of law, respect for human rights and fundamental freedoms, legislation concerning national security and criminal

[555] European Commission, *Political Declaration Setting out the Framework for the Future Relationship between the European Union and the United Kingdom (2019/C 384 I/02)* (OJ C 384I/178, 2019), 4, accessed June 25, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12019W/DCL(01)&from=EN.

[556] Article 45 GDPR.

[557] Christopher Kuner, "Developing an Adequate Legal Framework for International Data Transfers," in *Reinventing Data Protection*, ed. Serge Gutwirth et al. (Springer Netherlands, 2009), 263–273, accessed December 8, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1464323&download=yes.

law, the access of public authorities to personal data, security measures, rules on onward transfer, effective and enforceable data subject rights, the presence of one or more independent supervisory authorities that ensure and enforce compliance with data protection rules, and the international commitments the third country or international organization in question has entered into, especially in relation to the data protection field.

As it emerges from this list (which is much broader than the one under Article 25 DPD), the elements that should be considered by the European Commission when assessing the adequacy of the level of protection include not only the *content* of the data protection rules applicable in the given country or international organization but also the *procedural/enforcement mechanisms* in place to ensure the effectiveness of such rules. As explained by the A29WP in WP12,[558] in fact, when addressing the question "what constitutes 'adequate protection'?" under Article 25 DPD, attention should be directed to not only (1) the *content* of the rules applicable to the transferred data (content principles) but also (2) the *means* in place to ensure that such rules are enforced in practice (procedural/enforcement mechanisms). Substantive data protection rules and procedural/enforcement mechanisms should hence go hand-in-hand in order to make sure that complaints are investigated, that non-compliance is sanctioned and that individuals are afforded a right to redress.[559]

As for the second requirement (procedural/enforcement mechanisms), three main criteria should be taken into consideration when assessing the effectiveness of a data protection system in protecting personal data, namely:

1) The ability of a system "to deliver a good level of compliance with the rules": a good level of compliance relies on a high degree of awareness among controllers of their obligations, and of data subjects of their rights, on dissuasive sanctions, and on a system of verification by authorities or auditors.[560]

[558] Article 29 Data Protection Working Party, *WP12*.
[559] Ibid., 5.
[560] Ibid., 7.

2) The ability of a system "to provide support and help to individual data subjects in the exercise of their rights": institutional mechanisms should be in place so that complaints by data subjects can be investigated and their rights enforced.[561]

3) The ability of a system "to provide appropriate redress to the injured party where rules are not complied with": an independent adjudication or arbitration should be in place so that compensation can be paid to the injured party and sanctions can be imposed.[562]

The basic content principles and the basic procedural/enforcement mechanisms identified in WP12 and that should exist in order to conclude that a third country provides an adequate level of protection have been revised and updated by the A29WP in its 2017 opinion on adequacy referential (WP254).[563] The novelty in WP254 is that the A29WP has highlighted that when assessing the adequacy of the level of protection, the European Commission shall also take into consideration a third element, namely that the third country in question provides for some essential guarantees against access to data for law enforcement and national security purposes. In particular, the A29WP stressed that the four guarantees that it had previously identified in WP237 in the field of surveillance should also apply in the fields of law enforcement and national security: firstly, the processing or personal data "should be based on clear, precise and accessible rules"; secondly, "[n]ecessity and proportionality with regards to legitimate objectives pursued need to be demonstrated"; thirdly,

[561] Ibid.

[562] Ibid.

[563] Article 29 Data Protection Working Party, *Adequacy Referential (Updated) (WP254)*, 2017, accessed December 15, 2019, https://iapp.org/media/pdf/resource_center/wp254_Adequacy-referential_11-2017.pdf. As for content principles, the following elements should be present: basic data protection concepts and/or principles (e.g., the concepts of "personal data", "data controllers"; "data processor"); grounds for lawful and fair processing for legitimate purposes; purpose limitation principle; data quality and proportionality principle; data retention principle; security and confidentiality principle; transparency principle; right of access, rectification, erasure and objection; restrictions on onward transfers, and other additional content principles to be applied to specific types of processing (WP254, 5-7). As for the procedural and enforcement mechanisms, a system that is consistent with the EU framework should be characterized by the following elements: one or more independent supervisory authority should exist; the data protection system must ensure a good level of compliance; data controllers and those processing data on their behalf should be able to demonstrate compliance with the data protection framework (accountability); the data protection system must provide support and help to data subjects in the exercise of their rights and appropriate redress mechanisms shall be established (WP254, 8).

independent oversight should be in place; fourthly, individuals should be able to rely on effective remedies.[564]

As a result of the adequacy decision, data can flow freely to the "whitelisted" countries without any additional safeguards. Transfer of data to those countries is hence equated to intra-EEA transfers. The list of whitelisted countries now includes Andorra, Argentina, Canada,[565] Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the United States of America (limited to the Privacy Shield framework). Moreover, on 17 July 2018, Japan and the EU successfully concluded their discussion aimed at recognizing each other's data protection framework as equivalent[566] and on 23 January 2019, the European Commission has adopted the adequacy decision on Japan.[567] Adequacy talks are also ongoing with South Korea.[568]

Pursuant to Article 45(3), adequacy decisions shall be subject to "periodic review at least every four years".[569] Such a review shall take into account all the relevant developments in the third country or international organization concerned. The Commission shall also "monitor developments

---

[564] Ibid., 9.

[565] The adequacy decision concerning Canada is limited to organisations subject to the Canadian Personal Information Protection and Electronic Documents Act that applies to organizations that process personal data in the course of commercial activities.

[566] European Commission, *Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission* (Tokyo, 2018), accessed August 1, 2018, https://http://europa.eu/rapid/press-release_STATEMENT-18-4548_en.htmec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_4548.

[567] 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, 2019), (hereafter "EU-Japan Adequacy Decision").

[568] European Commission, "Adequacy of the Protection of Personal Data in Non-EU Countries," accessed May 26, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

[569] Article 45(3) GDPR. See also Recital 106 GDPR: "[t]hat periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources". As explained by the A29WP in WP254, the frequency of the review "must be adjusted to each third country or international organization with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule" (Article 29 Data Protection Working Party, *Adequacy Referential (Updated) (WP254)*, 4.). For instance, in its opinion on the Draft Implementing Decision on the adequate protection of personal data in Japan, the EDPB has invited the European Commission to conduct the review under Article 45(3) GDPR at least every two years. European Data Protection Board, *Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan*, 2018, 12, accessed December 15, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/2018-12-05-opinion_2018-28_art.70_japan_adequacy_en.pdf.

in third countries and international organizations that could affect the functioning of" adequacy decisions and, where necessary, "repeal, amend or suspend" existing adequacy decisions.[570] The Commission has also identified several criteria that it will consider when determining with which third country a dialogue on adequacy should be started:

> (i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
> (ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
> (iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
> (iv) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.[571]

5.4.2. The Safe Harbour and Its Invalidation

In order to allow the free flow of data between the EU and the US that is at the basis of the strong commercial relationship between the two regions, the European Commission adopted decision 2000/520/EC, the so-called Safe Harbour decision.[572] This decision was adopted under Article 25(6) of the 1995 Directive which empowered the European Commission to enter into negotiations with a third country with a view to remedying the situation that arise when the European Commission finds that that the third country concerned does not ensure an adequate level of protection. The Safe Harbour decision is hence the result of such negotiations with the US. By means of this decision, the European Commission recognized that the Safe Harbour Principles[573] and the accompanying frequently asked questions issued by the US Department of Commerce on 21 July 2000 ensured an "adequate level of protection" for personal data transferred to organisations established in the United States which were subject to the jurisdiction of the Federal Trade Commission or of the Department of Transportation.[574] Exceptions to these Principles were also allowed "to the extent necessary to

[570] Article 45(4)-(5) GDPR.

[571] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 8.

[572] European Commission, *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, 2000), (hereafter cited as Safe Harbour decision).

[573] Notice; choice; onward transfer; security; data integrity; access; enforcement.

[574] Article 1, Safe Harbour decision.

meet national security, public interest, or law enforcement requirements" and "by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization".[575]

The Safe Harbour regime was mainly relying on the commitments of the companies "established in the United States"[576] (meaning, not only US companies that provide services to the EU but also US subsidiaries of EU companies)[577] which had signed up to the Safe Harbour Principles. The Safe Harbour decision was hence a "partial" adequacy finding since it only applied to companies that had decided to commit to these Principles. The adherence to those Principles was voluntary but the rules were becoming binding for those organizations that decided to self-certify, i.e., declare to the Department of Commerce their commitment to adhere to the Principles.[578]

No detailed analysis of the Safe Harbour arrangement is necessary since it was invalidated by the ECJ in *Schrems*, where the Safe Harbour was deemed to be one of the conduits that allowed the NSA to access data transferred from the EU to the US.[579] The case in question was triggered by a complaint by Mr Schrems, an Austrian national, who contended that personal data of EU users should no longer be transferred from Facebook Ireland to the US servers belonging to Facebook Inc. since that country could not be deemed to ensure "true" adequacy following Snowden's revelations about

[575] Ibid., 10.

[576] Article 1, Ibid.

[577] European Commission, *Communication from the European Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM(2013) 847 final. (Brussels, 2013), 4–5, accessed April 26, 2019, https://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF.

[578] Safe Harbour decision, FAQ 6 –Self-Certification.

[579] However, the invalidation of the Safe Harbour was formally grounded upon the fact that Commission decision 2000/520/EC denied national supervisory authorities the power "to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him", in particular "where, in bringing such a claim, that person raises questions regarding the compatibility of a Commission decision adopted pursuant to Article 25(6) of that directive with the protection of the privacy and of the fundamental rights and freedoms of individuals" (*Schrems*, paragraph 99).

the mass surveillance programs conducted by the US intelligence services, and in particular by the NSA.

Several statements made by the ECJ in *Schrems* provide important guidance about the interpretation of the concept of "adequate level of protection", that, as seen above, has been retained under Article 45 GDPR: "the term 'adequate level of protection' must be understood as requiring the third country ... to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter".[580] In other words, although third countries are not required to grant a level of protection that is *identical* to the one within the EU framework, the essential requirements set out under the EU data protection legislation must be met.[581]

Against this background, the ECJ noted that, by including derogations from the Safe Harbour Principles, the Safe Harbour decision enables "interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States".[582] At the same time, the Safe Harbour decision "does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States" nor does the Safe Harbour decision "refer to the existence of effective legal protection against interference of that kind".[583]

The Safe Harbour framework was hence deemed by the ECJ to be at odds with the level of protection guaranteed within the EU where derogations and limitations to the right to respect for

[580] *Schrems*, paragraph 73 (italics mine).

[581] "Even though *the means* to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection *may differ* from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, *those means must* nevertheless *prove, in practice, effective* in order to ensure protection essentially equivalent to that guaranteed within the European Union". Ibid., paragraph 74 (italics mine).

[582] Ibid., paragraph 87.

[583] Ibid., paragraphs 88-89.

private life are allowed only in so far as they are strictly necessary.[584] In particular, legislation that allows "public authorities to have access on a generalised basis to the content of electronic communications" compromises the very essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the EU Charter of Fundamental Rights.[585] Likewise, legislation that does not provide for any legal remedy against the risk of abuse that may derive from such generalized access to personal data compromises the essence of the fundamental right to effective judicial protection enshrined in Article 47 of the Charter.[586]

5.4.3. From the Safe Harbour to the Privacy Shield

Following the invalidation of the Safe Harbour, further negotiations were started between the EU and the US in order to allow the flow of data between the two sides of the Atlantic. This discussion lead to the adoption of the Privacy Shield decision,[587] which, like the Safe Harbour, was adopted under the European Commission's powers under Article 25(6) DPD. This decision remains in force under the GDPR by virtue of Article 45(9) GDPR that prescribes that "[d]ecisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC", and among these decisions also the Privacy Shield, "shall remain in force until amended, replaced or repealed by a Commission Decision".[588] Overall, the Privacy Shield maintains the structure of the Safe Harbour but stronger obligations are established on US companies in order to incorporate the requirements laid out by the ECJ in *Schrems*. Like the Safe Harbour, the Privacy Shield sets out a system of self-certification whereby data can be freely transferred from the EU to "organizations in the United States"[589] which

[584] Ibid., paragraph 92. "Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail" (Ibid., paragraph 93).

[585] Ibid., paragraph 94.

[586] Ibid., paragraph 95.

[587] European Commission, *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* (OJ L 207/1, 2016), (hereafter cited as Privacy Shield decision).

[588] Article 45(9) GDPR.

[589] Article 1(3), Privacy Shield decision.

have voluntarily committed to the Principles (Privacy Shield participants). The Privacy Shield is constituted by the Principles[590] issued by the US Department of Commerce on 7 July 2016 and by official representations and commitments by several US agencies contained in the Annexes to the decision, including written assurance that access to data by US authorities for national security[591] and law enforcement purposes[592] is subject to specific limits and safeguards.

Like the Safe Harbour, the Privacy Shield includes explicit limitations to the Principles which are worded precisely in the same way as under the Safe Harbour.[593] The difference between the Safe Harbour and the Privacy Shield rests on the fact that, following the ECJ's ruling in *Schrems*, the Privacy Shield includes the findings of the European Commission on the limits that the US legal framework poses to access and use by US public authorities of the data transferred from the EU under the Privacy Shield framework.[594] On the basis of these findings, the European Commission concluded that

> *any interference* by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, *will be limited* to what is *strictly necessary* to achieve the legitimate objective in question, and that there exists effective legal protection against such interference.[595]

For the purpose of a brief analysis of the main differences between the Safe Harbour and the Privacy Shield, it is first worth recalling that the Privacy Shield Principles retain and further enhance the Safe Harbour Principles ("onward transfer" became "accountability for onward transfer", "data integrity" became "data integrity and purpose limitation", and "enforcement" became "recourse, enforcement and liability"). More specifically, under the recourse, enforcement and liability

[590] Notice; choice; accountability for onward transfer; security; data integrity and purpose limitation; access; recourse, enforcement and liability.

[591] See Letter from General Counsel Robert Litt (Office of the Director of National Intelligence), Privacy Shield decision, 91 ff.

[592] See Letter from Deputy Assistant Attorney General and Counselor for International Affairs Bruce Swartz, U.S. Department of Justice, Privacy Shield decision, 109 ff.

[593] Privacy Shield decision, 49.

[594] Ibid., Recitals 64-141. See also, Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 182–183.

[595] Privacy Shield decision, Recital 140 (italics mine).

principle, the Department of Commerce's oversight powers over the Privacy Shield have been enhanced and its cooperation with EU DPAs has been increased.[596] Moreover, the cooperation between Privacy Shield participants and DPAs has been strengthened.[597]

Possibilities of redress for the data subjects have also been improved: individuals can complain directly with the relevant self-certified organization;[598] independent recourse mechanisms, such as Alternative Dispute Resolution, are also made available to individuals at no cost;[599] individuals can also bring complaints to a DPA that will then channel the complaints to either the US Department of Commerce or the Federal Trade Commission;[600] the Federal Trade Commission also accepts complaints directly from individuals;[601] as a last resort, an arbitration option is made available to individuals (Privacy Shield Panel).[602] A new redress opportunity is also established for the first time against access to personal data for national security reasons (i.e., the EU-U.S. Privacy Shield Ombudsperson mechanism). The Ombudsperson mechanism is not limited to data transferred from the EU to the US pursuant to the Privacy Shield, but it also applies to data transferred through other legal bases.[603]

Attention will now be placed on the accountability for onward transfer principle since the purpose of onward transfer provisions is explicitly to avoid the anti-circumvention of the level of protection guaranteed under the EU data protection framework. Onward transfers are defined as "transfers of personal data from an organisation to a third party controller or processor, irrespective of whether the latter is located in the United States or a third country outside the United States (and the Union)".[604] As stated under Recital 27 of the Privacy Shield, the purpose of the rules on onward transfer "is to ensure that the protections guaranteed to the personal data of EU data subjects will not

[596] Ibid., 40-43.
[597] Ibid., 53-54.
[598] Ibid., 62. See also Recital 43.
[599] Ibid., 40 and 62. See also Recitals 40 and 45.
[600] Ibid., 43. See also Recitals 48-51.
[601] Ibid., Recital 54.
[602] Ibid., 45 and 62. See also Recital 42.
[603] Ibid., 72 ff..
[604] Ibid., Recital 27.

be undermined, and cannot be circumvented, by passing them on to third parties".[605] To achieve the said anti-circumvention objective, onward transfer can only take place on a basis of a contract that "provides the same level of protection as the one guaranteed by the Principles".[606]

From a more technical point of view, the Privacy Shield makes a distinction between transfer from the Privacy Shield participant (i.e., the original recipient) to a controller and transfer to a processor. Unlike the Safe Harbour which did not require any contract in the event of onward transfer to controllers, the Privacy Shield requires the Privacy Shield participant to enter into a contract with the third party controller in order to ensure that data will be processed "for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation".[607] The obligation to enter into a contract is, however, subject to an exception in the event that personal data are transferred between two controllers within a controlled group of corporations or entities. In such a case, in fact, transfer may be based "on *other instruments*, such as EU Binding Corporate Rules or other intra-group instruments (e.g., compliance and control programs), *ensuring the continuity of protection of personal information under the Principles*. In case of such transfers, the Privacy Shield organization remains responsible for compliance with the Principles".[608]

Onward transfer from the Privacy Shield Participant to a processor ("a third party acting as an agent") is also subject to stronger limitations compared to the Safe Harbour. More specifically, data

[605] Ibid., Recital 27.

[606] Ibid., Recital 28. See also Recital 29 under which "[t]he obligation to provide the same level of protection as required by the Principles applies to any and all third parties involved in the processing of the data so transferred irrespective of their location (in the U.S. or another third country) as well as when the original third party recipient itself transfers those data to another third party recipient, for example, for sub-processing purposes. In all cases, the contract with the third party recipient must provide that the latter will notify the Privacy Shield organisation if it makes a determination that it can no longer meet this obligation. When such a determination is made, the processing by the third party will cease or other reasonable and appropriate steps have to be taken to remedy the situation".

[607] Privacy Shield decision, 51. The Privacy Shield decision clarifies that the third-party controller that receives the data from the original recipient (i.e., the Privacy Shield participant) does not need to be a Privacy Shield organization. It is, in fact, the contract between the two controllers that "provides for the same level of protection as is available under the Privacy Shield" (Privacy Shield decision, 61).

[608] Ibid., 61 (italics mine).

should only be transferred for limited and specific purposes, the Privacy Shield participant must make sure that the processor is obligated to provide "at least the same level of privacy protection as is required by the Principles", and it is in charge of overseeing processor's compliance with the Principles.[609] Moreover, the "Privacy Shield organization shall remain liable under the Principles if its agent [i.e., processor] processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage".[610]

5.4.4. The Privacy Shield and the Risks of its Invalidation

Without further delving into what has changed and what has not from the Safe Harbour to the Privacy Shield,[611] it is important to highlight that the Privacy Shield is now facing serious invalidations risks. Two actions for annulment against the Privacy Shield decision have been lodged so far before the General Court. In *Digital Rights Ireland v Commission* (T-670/16), Digital Rights, a non-for-profit company, supported its claim about the invalidity of the contested decision by alleging, among others, that the decision is not in accordance with Article 25(6) DPD read in light of Articles 7 (Right to respect for private and family life), 8 (Right to respect for private and family life) and 47 (Right to an effective remedy and to a fair trial) of the Charter of Fundamental Rights of the European Union and of the *Schrems* decision.[612] Moreover, it alleged that "insofar as the contested

[609] Ibid., 51.

[610] Ibid., 52. On onward transfer see also, Hon and Millard, "How Do Restrictions on International Data Transfers Work in Clouds?," 265–266.

[611] For further information on the Privacy Shield decision see, among others, Doron S. Goldstein et al., "Understanding the EU-US 'Privacy Shield' Data Transfer Framework," *Journal of Internet Law* 20, no. 5 (2016): 18–22; Shona McCusker, "The EU-US Privacy Shield: The Antidote to the Transatlantic Data Transfer Headache?," *Business Law Review* 37, no. 3 (2016): 84–85; Emily Linn, "A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement Notes," *Vanderbilt Journal of Transnational Law* 50 (2017): 1311–1358; W. Gregory Voss, "The Future of Transatlantic Data Flows: Privacy Shield Or Bust?," *Journal of Internet Law* 19, no. 11 (2016): 9–18; Xavier Tracol, "EU–U.S. Privacy Shield: The Saga Continues," *Computer Law & Security Review* 32, no. 5 (October 1, 2016): 775–777; David Bender, "Having Mishandled Safe Harbor, Will the CJEU Do Better with Privacy Shield? A US Perspective," *International Data Privacy Law* 6, no. 2 (May 1, 2016): 117–138; Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems"; Shara Monteleone and Laura Puccio, *From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules* (European Parliamentary Research Service, 2017), accessed August 2, 2018, http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf.

[612] Action brought on 16 September 2016, *Digital Rights Ireland v Commission*, Case T-670/16, first and second plea in law.

decision allows, or in the alternative fails and has failed to safeguard against indiscriminate access to electronic communications by foreign law enforcement authorities, it is invalid as a breach of the Rights of Privacy, Data Protection ... as provided for under the Charter of Fundamental Rights of the European Union and by the general principles of EU Law".[613] In particular, the provisions under the US Foreign Intelligence Surveillance Act (FISA) as amended in 2008 allow US public authorities "to have secret access on a generalised basis to the content of electronic communications and consequently are not concordant with Article 47 of the Charter Fundamental Rights of the European Union".[614] The concerns expressed by the claimant were, however, not addressed by the General Court, which declared the action inadmissible without going to the substance of the case.[615]

The ECJ will still have an opportunity to rule upon the validity of the Privacy Shield decision in another case, *La Quadrature du Net and Others v Commission* (T-738/16). In this latter case, the applicant put forward similar pleas alleging, in particular, that the Privacy Shield decision infringes the Charter of Fundamental Rights of the European Union since it fails "to draw the conclusion that the US regulatory regime is in particular contrary to the essence of the fundamental right to respect for private life guaranteed by Article 7 of the Charter" despite the *generalized* nature of the collection of data allowed under the US regulatory regime.[616]

The A29WP has also expressed several doubts about the level of protection ensured under the Privacy Shield. In its First annual Joint Review adopted on 28 November 2017 (WP255), the A29WP has identified several unresolved issues both with reference to the commercial aspects of the Privacy Shield and with reference to the access by public authorities to personal data transferred from the EU to the US. As for the commercial aspects of the decision, the A29WP stressed, among other issues, the lack of clear information about the interpretation and application of the Principles, and about the

[613] Ibid., eighth plea in law.
[614] Ibid., fifth plea in law.
[615] Order of the General Court of 22 November 2017, *Digital Rights Ireland v Commission*, Case T-670/16, ECLI:EU:T:2017:838.
[616] Action brought on 25 October 2016, *La Quadrature du Net and Others v Commission*, Case T-738/16, first plea in law.

possibilities of redress for data subjects. The supervision over compliance with the Privacy Shield Principles should also be enhanced together with the self-certification process for companies in order to ensure "uninterrupted protection for data subjects".[617]

Moreover, and more generally, the A29WP noted that many obligations included in the Privacy Shield are not suitable to processors. Indeed, since processors, by definition, have no autonomy in determining the purposes and the means of the processing of personal data, the application of the Principles to processors may contradict the DP Agreement between the processor and the EU controller. For example, the DP Agreement may *not* authorize the onward transfer from the US processor to other third parties even when the conditions under the accountability for onward transfer principle are met. Full compliance with the notice principle may also raise challenges for processors since many of the requirements established under this principle are tailored to controllers. Under this principle, in fact, an organization must inform individuals, among others, about "the purposes for which it collects and uses personal information about them".[618] Processors would, however, be unable to provide for such a full notice since they do not determine the purposes of the data processing. The A29WP hence called for clarifications about the specific obligations that apply to processors.[619]

In WP255, the A29WP also raised several points of concern with reference to the access by public authorities to data transferred to the US. As for the access to data for national security purposes, the A29WP considered, among others, that the assertion by the US authorities that the US regulatory framework does not enable massive and indiscriminate collection of data for national security purposes is not sufficiently substantiated. The A29WP also expressed concerns with reference to

[617] Article 29 Data Protection Working Party, *WP255*, 2.

[618] Privacy Shield, 50.

[619] Article 29 Data Protection Working Party, *WP255*, 11–12. It should also be recalled that similar concerns about the application of the Privacy Shield Principles to processors were also expressed by A29WP a year earlier with reference to the Privacy Shield *draft* adequacy decision: "[w]ithout such clarification, the Principles could be interpreted and applied in a manner that offers too much control capacities to the Shield Agent [i.e., processor] and this would put the EU data exporter at risk of violating his obligations as a data controller under EU data protection law to which it is subject when transferring data to a Shield organisation acting as an Agent. In addition, this lack of clarity gives the impression that the processor might reuse the data as he wishes". Article 29 Data Protection Working Party, *WP238*, 16.

access to data for law enforcement purposes, especially regarding the effectiveness of the available remedies for individuals in case of such access. Moreover, in the light of Article 47 of the Charter of Fundamental Rights of the European Union, the powers of the Ombudsperson mechanism were deemed by the A29WP not sufficient to guarantee effective remedy against unlawful access by intelligence agencies.[620] In this regard, it should be recalled that on 5 July 2018, the US Ombudsperson was invited for an exchange with the EDPB on the occasion of its Second plenary meeting. Although the meeting was considered "interesting", the EDPB concluded that the Ombudsperson did not provide any "conclusive answer" to the concerns expressed by the A29WP and called for "supplementary evidence to be given by the US authorities in order to address these concerns".[621]

The progress made in the Privacy Shield were also deemed insufficient by the EDPS in its 2016 Opinion on the Privacy Shield draft adequacy decision.[622] In this opinion, the EDPS stressed that the benchmark against which the Privacy Shield Framework should be assessed is not the previously invalidated Safe Harbour decision but the EU legal framework. In the light of this, the EDPS noted that "notwithstanding recent trends to move from indiscriminate surveillance on a general basis to more targeted and selected approaches, the scale of signals intelligence and the volume of data transferred from the EU subject to potential collection once transferred and notably when in transit, is likely to be still high and thus open to question".[623] And the Privacy Shield "may be interpreted as legitimising this routine".[624] In order to avoid this undesirable consequence, the

[620] Article 29 Data Protection Working Party, *WP255*, 14–20.

[621] European Data Protection Board, Second plenary meeting, July 5, 2018, accessed August 2, 2018, https://edpb.europa.eu/news/news/2018/european-data-protection-board-second-plenary-meeting-icann-psd2-privacy-shield_en.

[622] European Data Protection Supervisor, *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*.

[623] Ibid., 6–7.

[624] Ibid., 7. Similar concepts have been expressed by the EDPS in March 2018: "Yet we continue lack precise information about mass surveillance in practice. The Privacy Shield cannot be viewed as a legitimation of routine access by the authorities of any state, in the EU or elsewhere, to the personal data of EU individuals. We need a more comprehensive map of the legal bases used for data processing for law enforcement and intelligence purposes so that independent supervisory authorities can make a proper assessment". Giovanni Buttarelli, "The EU-U.S. Privacy Shield Two Years On," *European Data Protection Supervisor*, last modified March 26, 2018, accessed May 30, 2018, https://edps.europa.eu/press-publications/press-news/blog/eu-us-privacy-shield-two-years_en.

EDPS recommended a better clarification of the exceptions to the Principles: the ECJ in *Schrems* "required clear and precise rules limiting the scope and application of any interference with fundamental rights". This is why the Privacy Shield should better clarify under what conditions derogations can be invoked.[625]

Further changes were suggested by the EDPS with reference to the commercial aspects of the Privacy Shield: the data minimisation and the data retention principles should be fully integrated while the purpose limitation principle should be clarified; additional safeguards should be included with reference to automated processing; redress mechanisms and oversight should also be enhanced,[626] and the inclusion of new elements first introduced under the GDPR such as the principles of privacy by design, privacy by default and data portability should be considered.[627] Overall, the EDPS severely questioned the longevity of the Privacy Shield by recommending the European Commission, "[r]egardless of any final changes to the draft ... to timely identify relevant steps for *longer term* solutions to *replace the Privacy Shield*, if any, with *more robust* and *stable* legal frameworks to boost transatlantic relations".[628]

The European Parliament also voiced its concerns on several occasions. In 2016, in its resolution on transatlantic data flow,[629] the European Parliament noted that bulk collection of data is still permitted under the US law. Such generalized collection of data "does not meet the stricter criteria of necessity and proportionality as laid down in the Charter".[630] Moreover, the appointment of an Ombudsperson seems insufficient to grant effective legal remedy against unlawful government surveillance.[631] In April 2017, in its resolution on the adequacy of the protection afforded by the EU-

[625] European Data Protection Supervisor, *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, 8.
[626] Ibid., 9–10.
[627] Ibid., 12.
[628] Ibid., 3 (italics mine).
[629] European Parliament, *Resolution of 26 May 2016 on Transatlantic Data Flows* (2016/2727(RSP), 2016), accessed August 2, 2018, https://www.europarl.europa.eu/doceo/document/TA-8-2016-0233_EN.pdf?redirect.
[630] Ibid., paragraph 4.
[631] Ibid., paragraph 8.

US Privacy Shield,[632] the European Parliament reiterated that several unresolved issues still affect the Privacy Shield framework with reference to both commercial aspects and access to data for law enforcement and national security purposes. Among others, the Privacy Shield lacks rules on automated decision making and on a general right to object; no explicit principles are laid out with reference to processors; bulk collection of data is still permitted; not all legal bases that US authorities can use to access data are covered by a possibility to redress for individuals; and, as already stressed in its 2016 resolution, the Ombudsperson mechanism is inadequate in providing effective redress to EU individuals. Overall, these concerns "could lead to a *fresh challenge* to the decision on the adequacy of the protection being brought before the courts in the future".[633]

The motion for a resolution that the LIBE Committee presented in April 2018[634] shows that the concerns of the European Parliament about the weaknesses of the Privacy Shield have been exacerbated in the light of further events. In particular, with reference to the commercial aspects of the Privacy Shield, "[i]n view of the recent revelations of misuse of personal data by companies certified under the Privacy Shield such as Facebook and Cambridge Analytica", the European Parliament called on the US authorities "to enforce the Privacy Shield to act upon such revelations without delay in full respect with the assurances and commitments given to uphold the current Privacy Shield arrangement and if needed, to remove such companies from the Privacy Shield list".[635] With reference to law enforcement and national security issues, the European Parliament noted that "the reauthorisation of section 702 of the FISA act", which allows the acquisition of foreign intelligence

[632] European Parliament, *Resolution of 6 April 2017 on the Adequacy of the Protection Afforded by the EU-US Privacy Shield* (2016/3018(RSP), 2016), accessed August 2, 2018, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0131_EN.pdf?redirect.

[633] Ibid., paragraph 11 (italics mine).

[634] European Parliament and Committee on Civil Liberties Justice and Home Affairs, *Draft Motion for a Resolution, to Wind up the Debate on the Statement by the Commission Pursuant to Rule 123(2) of the Rules of Procedure on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield* (2018/2645(RSP), 2018), accessed August 2, 2018, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf.

[635] Ibid., paragraph 10.

information about *non-US* persons located *outside* the US, "for 6 more years calls into question the legality of the Privacy Shield".[636] Moreover, the European Parliament

> Express[ed] its strong concerns regarding the recent adoption of the Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943), which expands the abilities of American and foreign law enforcement to target and access people's data across international borders without making use of the instrument of Mutual legal Assistance (MLAT) instruments, which provide for appropriate safeguards and respect the judicial competences of the countries where the information is located;[637]

According to the European Parliament, a more "balanced solution" than the adoption of the Cloud Act would have been the strengthening of the existing MLAT regime.[638]

Even stronger words were chosen by the European Parliament in its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield,[639] where it took "the view that the current Privacy Shield arrangement does not provide the adequate level of protection required by Union data protection law and the EU Charter as interpreted by the" Court of Justice of the European Union[640] and, in the event of persistent non-compliance with the EU standards by the US, it called "on the Commission to *suspend* the Privacy Shield until the US authorities comply with its terms".[641]

Despite these widespread criticisms,[642] the European Commission, in its first annual review of the functioning of the EU–U.S. Privacy Shield released on 18 October 2017, has concluded that "the United States continues to ensure an adequate level of protection for personal data transferred

---

[636] Ibid., paragraph 16.

[637] Ibid., paragraph 18.

[638] Ibid., paragraph 19.

[639] European Parliament, *Resolution of 5 July 2018 on the Adequacy of the Protection Afforded by the EU-US Privacy Shield* (2018/2645(RSP), 2018), accessed February 12, 2019, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf?redirect.

[640] Ibid., paragraph 34.

[641] Ibid., paragraph 35 (italics mine).

[642] See also the comment from Monique Goyens, Director General of The European Consumer Organisation: "[i]t is disappointing that the EU is showing so little appetite for defending its pioneering data protection rules. Consumers usually do not know or control where companies are sending their personal data. Their privacy rights should not be weakened just because data is transferred to the US or elsewhere. Whenever personal data travels across borders, it must also be protected across borders". The European Consumer Organization (BEUC) - Press Release, "Privacy Shield Opens Hole in Protection of EU Citizens' Privacy," last modified July 12, 2016, accessed August 3, 2018, https://www.beuc.eu/publications/beuc-pr-2016-011_privacy_shield_-_adequacy_agreement.pdf.

under the Privacy Shield from the Union to organisations in the United States".[643] This conclusion was confirmed by the European Commission one year later in its second annual review with reference to both the commercial aspects of the framework and the aspects concerning the access to personal data by the US public authorities. With reference to the latter aspects, however, the absence of a permanent Privacy Shield Ombudsperson was identified by the European Commission as a matter of serious concern. The European Commission will, in fact, "consider taking appropriate measures" under the GDPR if a nominee is not identified by the US government by 28 February 2019.[644] In response to this pressure, in January 2019, the US administration announced its intention to appoint Keith Krach as the permanent Ombudsperson under the Privacy Shield.[645]

Several improvements were also acknowledged by the representatives of the EDPB which took part to the European Commission's second annual review.[646] However, the EDPB stressed that several points of concerns and uncertainties that have been expressed by the A29WP in its previous opinions still affect both the commercial aspects of the Privacy Shield (e.g., the checks conducted by the US authority on companies' compliance with the Privacy Shield Principles are mainly focused on formal aspects rather than on the substance of the Principles; the area of onward transfers remains problematic) and the derogations to the Privacy Shield Principles to permit access to data for law enforcement and national security purposes (e.g., massive and indiscriminate access to data remains

[643] 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. (Brussels, 2017), 4, accessed April 26, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0611&from=EN.

[644] European Commission, *Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*, COM(2018) 860 final. (Brussels, 2018), 5–6, accessed April 26, 2019, https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf.

[645] "AmCham EU Welcomes Announcement to Nominate Privacy Shield Ombudsperson," *AmCham EU*, last modified January 24, 2019, accessed April 27, 2019, http://www.amchameu.eu/news/amcham-eu-welcomes-announcement-nominate-privacy-shield-ombudsperson; Amanda Lee, "US to Appoint Permanent Privacy Shield Ombudsperson, as EU Pressure Tells," *Euractiv.Com*, January 23, 2019, accessed April 27, 2019, https://www.euractiv.com/section/data-protection/news/us-to-appoint-permanent-privacy-shield-ombudsperson-following-eu-pressure/; "President Donald J. Trump Announces Intent to Nominate Individual to Key Administration Posts," *The White House*, accessed April 27, 2019, https://www.whitehouse.gov/presidential-actions/president-donald-j-trump-announces-intent-nominate-individual-key-administration-posts/.

[646] As foreseen under Recital 147 of the Privacy Shield decision, the meetings that the Commission arranges with the US authorities in order to perform the Annual Joint Review of the Privacy Shield are open to representatives of the Article 29 Working Party.

an issue; the redress by EU citizens before US courts is not effectively guaranteed; the powers of the Ombudsperson to remedy violations perpetrated by intelligence authorities do not meet the high threshold under Article 47 of the EU Charter).[647]

A positive conclusion was also reached by the European Commission in its third annual review which took place in September 2019.[648] Indeed, the findings of the European Commission confirm the adequacy of the Privacy Shield with reference to both the commercial aspects and the aspects related to the access to data by public authorities. As for the commercial aspects, the European Commission acknowledged and welcomed the progress made by the Department of Commerce in ensuring effective compliance with the Privacy Shield Principles and the fact that some enforcement actions have been concluded by the Federal Trade Commission for the violations of the Principles. The European Commission also welcomed the explanations given by the US authorities on the access to personal data for law enforcement and national security purposes which confirmed the European Commission's finding in the adequacy decision.[649] On this point, however, it noted that "once the Court rules on the pending [*Schrems II* case], the Commission may have to reassess the situation".[650] At the same time, the European Commission identified some steps that should be taken so as to boost the effectiveness of the framework, for example, by strengthening the oversight over compliance with the accountability for onward transfers principle, by developing tools to detect false claims of participation in the Privacy Shield, and by boosting information sharing between the Federal Trade Commission and the EU DPAs.[651]

The longevity of the Privacy Shield seems hence to be highly dependent on future developments both within the US framework, that the European Commission will continue to closely

[647] European Data Protection Board, *EU-U.S. Privacy Shield - Second Annual Joint Review*, 2019, accessed December 15, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf.

[648] European Commission, *Report from the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield* (Brussels, 2019), accessed December 8, 2019, https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf.

[649] Ibid., 3–7.

[650] Ibid., 3.

[651] Ibid., 8.

monitor in order to verify the continuity of the adequacy finding, and within the EU framework, where, as seen above, the Privacy Shield decision is currently facing the risk of being invalidated by the EU General Court. Against this background, national data protection authorities may not consider the Privacy Shield (alone) as a sufficiently solid legal basis for lawfully transferring data to third countries[652] and controllers may prefer resorting to other transfer mechanisms.[653] Moreover, it should be noted that these concerns do not affect solely the Privacy Shield but also other adequacy decisions. In WP241,[654] in fact, the A29WP regretted that in amending the draft adequacy decisions regarding other countries[655] (including Canada, Switzerland, Argentina, the State of Israel, the Eastern Republic of Uruguay and New Zealand) in the light of *Schrems,* the Commission did "not carried out an in-depth assessment of the conditions under which public authorities in the third countries concerned

[652] With specific reference to security measures, for example, in WP196, the A29WP noted that "the Safe Harbor principles *by themselves* may ... *not guarantee* the data exporter the *necessary means* to ensure that *appropriate security measures* have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC" (Article 29 Data Protection Working Party, *WP196*, 18, italics mine.). This alludes to the need to complement the Safe Harbour principles with some additional measures, possibly even SCCs or BCRs (Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 199–200.) In the same vein, in 2012, the Hungarian DPA opposed the transfer of personal data to a cloud computing service provider whose parent company was registered in the US. Indeed, although the service provider had self-certified under the Safe Harbour framework, according to the Hungarian DPA "the sensitive nature of the personal data" involved in the case in question significantly increase[d] the security concerns". In the case examined, the data controller was a political association who wished to process the personal data of its supporters via a cloud computing service provider (Article 29 Data Protection Working Party, *Sixteenth Report – Covering the Year 2012*, 2014, 62, accessed December 15, 2019, https://cnpd.public.lu/dam-assets/en/publications/rapports/groupe29/16th_annual_report_en.pdf.).

[653] "... Controllers may come to the conclusion that the best approach for them is to utilize standard contractual clauses instead of the Privacy Shield to transfer data". Ariel Silverstone et al., "European Parliament Voted to Suspend Privacy Shield: Now What?," *Iapp*, September 25, 2018, accessed January 14, 2019, https://iapp.org/news/a/european-parliament-voted-to-suspend-privacy-shield-now-what/. "... [T]he Privacy Shield does not give companies absolute legal certainty when transferring personal data to the US. Due to the uncertain future of the Shield, companies are advised to regularly review their own policies on international data transmission and consider other options. This is the only way to be prepared should there be sudden changes to the current system". "With the Future of the US-EU Data Privacy Shield in Doubt, Companies Are Considering Other Options," *CMS*, last modified October 29, 2018, accessed January 17, 2019, https://www.cms-lawnow.com/ealerts/2018/10/with-the-future-of-the-us-eu-data-privacy-shield-in-doubt-companies-are-considering-other-options.

[654] Article 29 Data Protection Working Party, *Opinion 04/2016 on European Commission Amendments Proposals Related to the Powers of Data Protection Authorities in Standard Contractual Clauses and Adequacy Decisions (WP241)*, 2016, accessed December 15, 2019, https://iapp.org/media/pdf/resource_center/wp241_Opinion-EC_DPAs-SCCs-adequacy.pdf.

[655] European Commission, *Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 Amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the Adequate Protection of Personal Data by Certain Countries, Pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council 25(6) of Directive 95/46/EC of the European Parliament and of the Council* (OJ L 344/83, 2016).

access personal data transferred on the basis of the relevant decisions on adequacy".[656] This "could jeopardize their legal validity possibly leading to a referral to a competent Court".[657]

Several concerns have also been voiced by the EDPB with reference to the draft EU-Japan adequacy decision both with reference to the commercial aspects of the decision and the aspects related to the access to the transferred data by the Japanese public authorities. As for the commercial aspects of the decision, the EDPB has expressed concerns, among others, with reference to onward transfers of personal data; it noted that the notion of "consent" as a basis for processing and for transferring data does not include the right to withdrawal, and other key concepts of the Japanese data protection legislation are unclear. Moreover, in the view of the EDPB, the Japanese redress mechanisms in the event of complaint may be hardly accessible since the support system is only available in Japanese.[658] The EDPB also welcomed clarifications on the procedures and the measures for accessing data in the field of law enforcement and of national security.[659]

Similar concerns about the adequacy of the level of data protection afforded by the Japanese legal framework have also been expressed by the European Parliament.[660] Among others, the European Parliament noted that the definition of personal data under Japanese data protection law is narrower than the one adopted under the GDPR and this might create room for potential loopholes since personal data within the meaning of the GDPR may fall outside the scope of the Japanese legislation;[661] it pointed out the lack in the Japanese framework of a comprehensive system of protection against automated decision-making and profiling;[662] it invited the European Commission to assess whether the fact that business operators can voluntarily hand data over to law enforcement

[656] Article 29 Data Protection Working Party, *WP241*, 4. In particular, the A29WP regretted that in amending the adequacy decisions in the light of *Schrems*, the Commission only addressed ECJ's conclusion on the powers of the DPAs.

[657] Ibid.

[658] European Data Protection Board, *Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan*, 13–24.

[659] Ibid., 24–41.

[660] European Parliament, *Resolution of 13 December 2018 on the Adequacy of the Protection of Personal Data Afforded by Japan* (2018/2979(RSP), 2018), accessed January 14, 2019, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0529_EN.html?redirect.

[661] Ibid., paragraphs 13-16.

[662] Ibid., paragraph 17.

agencies is compatible with the GDPR framework;[663] and it "is seriously worried" that the mass surveillance activities conducted by the Japanese public authorities that have been unveiled by some media reports "will not stand the test of the criteria established by the European Court of Justice in the Schrems judgment".[664] However, as seen above, these concerns did not stop the European Commission from adopting the adequacy decision on Japan on 23 January 2019, thus "creating the world's largest area of safe data flows".[665]

5.4.5. Other (Structural) Problems

In addition to the uncertainties about the legal validity of the existing adequacy decisions that have been analysed above, adequacy decisions as a legal basis for transfer also suffer from some structural problems. First and foremost, the process to determine adequacy is notoriously lengthy[666] and only a few countries have been whitelisted so far so that the practical relevance of adequacy findings as a legal basis for transfer is limited. At the same time, as it will be argued in the next chapter (6.2.5.), it should be noted that the fact that many States have started to implement DPD/GDPR-like data protection legislations may foster the adoption of adequacy decisions.

Moreover, the focus on territory implies that adequacy decisions only allow transfer of data to the *territories* of the whitelisted countries, while transfer of data to entities (*recipients*) subject to the jurisdiction of whitelisted countries which, in turn, make use of data centres located in non-whitelisted countries would not be covered by the adequacy decisions. This focus on the territory makes adequacy decisions particularly ill-suited to regulate transfers in the cloud where data are transferred and processed in different geographical locations. As noted by the A29WP in WP196,

---

[663] Ibid., paragraph 23.

[664] Ibid., paragraph 24.

[665] European Commission - Press release, "European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows," last modified January 23, 2019, accessed May 10, 2019, http://europa.eu/rapid/press-release_IP-19-421_en.htm.

[666] United Nations Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 2016, 14, accessed August 3, 2018, http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf; Hogan Lovells, *International Data Transfers. Considering Your Options*, 2015, accessed August 2, 2018, https://www.hldataprotection.com/files/2015/10/HL-International-Data-Transfers-Considering-your-options.pdf.

"[a]dequacy findings, including Safe Harbor, are limited in respect of the geographical scope, and therefore do not cover all transfers within the Cloud".[667] Notably, the adequacy decision concerning Canada seems to be an exception to this approach. Article 1 of Commission decision 2002/2/EC, in fact, prescribes that "[f]or the purposes of Article 25(2) of Directive 95/46/EC, Canada is considered as providing an adequate level of protection for personal data transferred from the Community to *recipients subject to the Personal Information Protection and Electronic Documents Act*"[668] (PIPEDA). This adequacy decision seems hence to place the focus on the jurisdiction to which the data recipient is subject rather than on the location of the recipient.[669]

5.5. Appropriate Safeguards

5.5.1. The Implementation of Contractual Solutions between the EEA Data Exporter and the non-EEA Data Importer

5.5.1.1. General Remarks

In the absence of an adequacy decision pursuant to Article 45, Article 46 GDPR allows for international data transfers when the controller or the processor has provided "appropriate safeguards" by means, among others, of contractual solutions. The possibility to use contracts as a legal basis for international transfers of personal data was also offered under Article 26 of the DPD. The GDPR has, however, introduced some novelties in the existing framework by expanding the applicability of SCCs that can now be included in contracts between EEA processors and non-EEA

[667] Article 29 Data Protection Working Party, *WP196*, 17. See also, Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 158–159; Hon and Millard, "How Do Restrictions on International Data Transfers Work in Clouds?," 264–265.

[668] Article 1, European Commission, *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 (2002/2/EC)* (OJ L 2/13, 2001), (italics mine).

[669] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 158.

processors,[670] by offering new contractual solutions under Article 46(2)(d) and, in some cases, by abolishing the need for prior authorization by national data protection authorities.[671]

Certainly, contracts are also used as a basis for transfers of data *within* the European Union (i.e., DP Agreements pursuant to Article 17 DPD, now Article 28 GDPR). However, the A29WP has in several occasions stressed that contractual obligations for intra-EEA transfers differ substantially from contractual solutions that need to be implemented in the event of international data transfer. Indeed, as noted by the A29WP back in 1998 (WP12), in the event of intra-EEA data flow, contracts between data controllers and data processors aim "to define and regulate the split of data protection responsibilities when more than one entity is involved in the data processing in question": the data controller will be responsible for complying with EU data protection legislation, while the processor will only be responsible for data security.[672]

On the other hand, when entities in third countries are involved, in addition to determining how the data protection responsibility should be divided between the two entities, the contract "must provide *additional safeguards* for the data subject made necessary by the fact that the recipient in the third country is not subject to an enforceable set of data protection rules providing an adequate level of protection". In other words, contractual provisions "must satisfactorily *compensate for the absence* of a *general level of adequate protection*, by including the essential elements of protection which are missing in any given particular situation".[673] To satisfy this aim, the adequacy of contractual solutions

---

[670] "Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) contractual clauses between the controller or *processor and* the controller, *processor* or the recipient of the personal data in the third country or international organization; ...". Article 46(3)(a) GDPR (italics mine).

[671] Article 46(2) GDPR.

[672] Article 29 Data Protection Working Party, *WP12*, 15–16.

[673] Ibid., 16 (italics mine). See also, Article 29 Data Protection Working Party, *Working Document: Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries (WP9)*, 1998, 11, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp9_en.pdf.: "[c]ontracts are used within the Community as a means of specifying the split of responsibility for data protection compliance between the data controller and a sub-contracted processor. When a contract is used in relation to data flows to third countries it must do much more: it must provide additional safeguards for the data subject made necessary by the fact that the recipient in the third country is not subject to an enforceable set of data protection rules providing an adequate level of protection". This concept was reiterated in Article 29 Data Protection Working Party, *WP47*.: "...the Working Party would like to stress the fact that the data controller's compliance with national provisions adopted pursuant Article 17 of Directive 95/46/EC does not constitute, *per se*, the exercise described in Article 26 (2) of the Directive, that is, to adduce sufficient safeguards that could lead a Member State to

in protecting transferred data should be assessed on the basis of the same elements that are taken into account when assessing the level of adequacy offered in a third country under Article 25 DPD, now Article 45 GDPR: (1) substantive data protection rules and (2) procedural/enforcement mechanisms whereby those rules can be enforced in practice.[674]

Contractual solutions should hence include a full set of data protection principles that the non-EEA data recipient shall apply to the processing of the transferred data (first requirement), together with the means that make such rules effective (the second requirement) (5.4.1.). As for the second requirement (procedural/enforcement mechanisms), the same criteria that are applied to assess the effectiveness of a data protection system provided by a third country under Article 45 GDPR shall also apply in assessing the effectiveness of contractual solutions in protecting data:

1) The ability of contractual solutions to deliver a good level of compliance: when it comes to contractual solutions, ensuring a sufficient level of compliance on the part of the non-EEA data recipient is particularly challenging since liability directly rests with the EEA data exporter while only an indirect liability would rest with the non-EEA data recipient. Such indirect liability derives from the fact that, in the event of sanctions, the EEA data exporter could recover any losses by bringing a legal action against the non-EEA data recipient. However, such indirect liability may not be sufficiently dissuasive for the non-EEA data importer so that some form of external inspection of the processing activities conducted by the data recipient, like audits, may be necessary.[675]
2) The ability of contractual solutions to provide support and help to data subjects: ensuring that data subject's complaints are effectively investigated is particularly challenging when data are transferred to third countries on the basis of contractual solutions since the investigative powers of national data protection authorities are confined within their territorial borders.

authorise a transfer or a set of transfers within the meaning of Article 26 (2), because these contracts need to supply for the lack of adequate protection in the country of destination which is not the purpose of Article 17 of Directive 95/46/EC" (2-3, paragraph 2).

[674] Article 29 Data Protection Working Party, *WP12*, 17 and 23.

[675] Ibid., 21.

Indeed, when data are transferred to third countries, Member States' DPAs cannot rely on the same system of mutual assistance that has been established within the EU. In order to overcome these inherent "territorial" limitations of DPA's monitoring and investigative powers, a specific clause could be included in the contract under which the non-EEA data importer agrees to be audited by the DPA of a Member State when non-compliance with the EU data protection principles is suspected.[676]

3) The ability of contractual solutions to provide redress to injured data subjects: some legal solutions need to be devised in order to ensure that the data subject can benefit from appropriate legal remedy, for example by allowing the data subject to claim rights under the contract between the data exporter and the data importer, or by making sure that the EEA data exporter remains liable for any damage that may be caused by an unlawful processing conducted by the non-EEA data recipient.[677]

Overall, it is clear that the transfer of data to a non-EEA recipient raises several problems that do not arise when data are transferred within the EEA since the physical distance between the data exporter and the data recipient makes the enforcement of the contractual obligations and of the decisions of the Member States' DPA "considerably more difficult" and thereby exposes data subjects to higher risks.[678]

Another crucial problem that arises when data are transferred to entities in third countries is the "problem of overriding law". The non-EEA data recipient may, in fact, be required by the law to which it is subject to disclose data to public authorities, like law enforcement authorities, and those legal requirements "might take precedence over any contract to which the processor [i.e., the data recipient] is subject".[679] Certainly, similar requests may be also put forward by public authorities within the EEA. However, under the EU data protection framework, such requests must be limited to

[676] Ibid., 20.
[677] Ibid., 18–19.
[678] Article 29 Data Protection Working Party, *WP47*, 3 (paragraph 2).
[679] Article 29 Data Protection Working Party, *WP12*, 21.

what is necessary in a democratic society.[680] To the contrary, in countries outside the EEA, "similar limitations on the ability of the state to require the provision of personal data from companies and other organisations operational on their territory may not always be in place".[681] The same problem was also identified in WP38, where the A29WP noted that "[m]andatory legislation applicable to the Data Importer *prevails over his contractual obligations* and there could be situations where the Data Importer may be compelled not to respect all the data protection rules included in the contract".[682] Similarly, in WP47, the A29WP highlighted that "there is always the possibility of data processors in third countries being subject to *public interventions* which might *go beyond what is necessary in a democratic society*".[683]

5.5.1.2. Standard Contractual Clauses

The GDPR has inherited from the 1995 Directive the possibility to frame international data transfers on the basis of standard contractual clauses, i.e., contracts between EEA data exporters and non-EEA data importers which aim to regulate the transfer of data between the two entities, their respective obligations and liabilities, and third-party beneficiary rights (i.e., the rights that data subjects can exercise against the data exporter, the data importer and, sometimes, even against sub-processors). In addition to the SCCs adopted by the European Commission,[684] the GDPR has

[680] Under Article 23(1) GDPR, "Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard", among others, "(a) national security; (b) defence; (c) public security; (d) 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; ...". See also Article 29 GDPR under which the "processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, *unless required to do so by Union or Member State law*" (italics mine). Similar provisions were included under Article 13(1) and 16 of the 1995 Directive.

[681] Article 29 Data Protection Working Party, *WP12*, 21.

[682] Article 29 Data Protection Working Party, *Opinion 1/2001 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Article 26(4) of Directive 95/46 (WP38)*, 2001, 3 (italics mine), accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp38_en.pdf.

[683] Article 29 Data Protection Working Party, *WP47*, 3 (paragraph 2, italics mine). See also, Article 29 Data Protection Working Party, *WP9*, 10.

[684] Article 46(2)(c) GDPR.

expanded the applicability of SCCs by prescribing that they may also be adopted by national supervisory authorities (and then approved by the European Commission),[685] thus offering a "national alternative" to the SCCs adopted by the European Commission.[686] How this (new) mechanism for data transfer will develop in practice is yet to be seen.

The European Commission has adopted two sets of SCCs for transfers from an EEA controller to a non-EEA controller ("2001 SCCs" adopted with decision 2001/497/EC and "2004 SCCs" adopted with decision 2004/915/EC)[687] and one set of SCCs for transfers from an EEA controller to a non-EEA processor ("2010 SCCs" adopted with decision 2010/87/EU).[688] These decisions remain valid under the GDPR by virtue of Article 46(5) GDPR under which "[d]ecisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary".[689] Since their adoption, SCCs have not been updated in the light of the most recent developments and of the adoption of the GDPR in the first place. However, in its position and findings on the application of the GDPR of 19 December 2019, the Council has encouraged the Commission to revise these clauses so as "to take into account the needs of controllers and processors".[690] It is also worth recalling that the need for two separate sets of SCCs depending on whether the data importer is a non-EEA processor or a non-EEA controller derives from the fact

---

[685] Article 46(2)(d) GDPR.

[686] Detlev Gabel and Tim Hickman, "Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation," *White & Case LLP International Law Firm*, last modified September 13, 2017, accessed January 16, 2019, https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection.

[687] European Commission, *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, 2001); European Commission, *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 (2004/915/EC)* (OJ L 385/74, 2004).

[688] European Commission, *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 (2010/87/EU)*.

[689] Article 46(5) GDPR.

[690] Council of the European Union, *Council Position and Findings on the Application of the General Data Protection Regulation (GDPR)* (Brussels, 2019), 9 (paragraph 19), accessed December 29, 2019, https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf. This position was adopted pursuant to Article 97 GDPR under which by "25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council". In carrying out its reviews, "the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources".

that transfers of data to non-EEA processors "do not require the same safeguards because the processor acts exclusively on behalf of the controller".[691]

It should also be noted that 2010 SCCs only apply to transfers from EEA controllers to non-EEA processors while they do not apply when data are transferred from an EEA controller to an EEA processor and then to a non-EEA processor.[692] Simply put, 2010 SCCs cannot be deployed to frame transfer in the following situation:

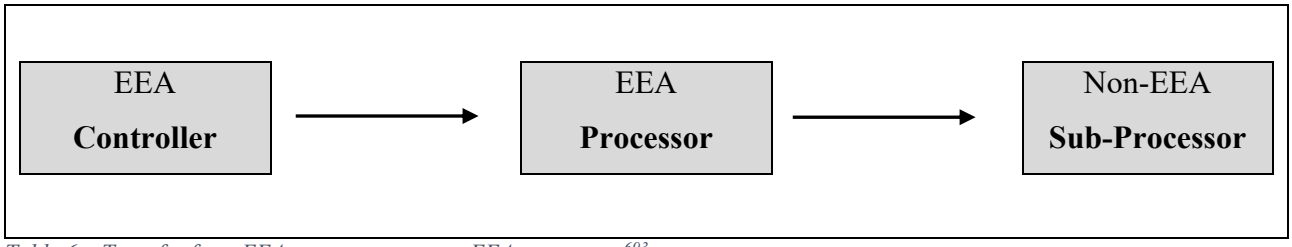

Table 6 – Transfer from EEA processors to non-EEA processors[693]

In a similar scenario, in order to regulate the transfer from the EEA processor to the non-EEA processor, the A29WP has identified three different possibilities: "a. Direct contracts between EEA-based controllers and non-EEA-based processors; b. Clear mandate from EEA-based controllers to EEA-based processors in order to use Model Clauses 2010/87/EU in their name and on their behalf; c. Ad-hoc contracts".[694] In the first case (solution a.), the SCCs are signed between the EEA controller and the non-EEA processor while the relationship between the EEA controller and the EEA processor is regulated by the service provider agreement which also includes the DP Agreement pursuant to Article 17 DPD/28 GDPR. In the second case (solution b.), the service provider agreement between the EEA controller and the EEA processor also includes the mandate to the EEA processor to enter into SCCs with the non-EEA processor. The EEA controller remains the data exporter while the non-EEA sub-processor is the data importer. Lastly (solution c.), ad-hoc contracts can be implemented.

[691] Recital 8, Commission decision 2001/497/EC.
[692] Recital 23, Commission decision 2010/87/EU.
[693] This table reproduces the table in Article 29 Data Protection Working Party, *FAQs in Order to Address Some Issues Raised by the Entry into Force of the EU Commission Decision 2010/87/EU 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 (WP176)*, 2010, 3, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf.
[694] Ibid., 4.

These contracts shall contain the same principles and safeguards that are included in SCCs. DPAs will retain the power to review these contracts and authorize transfers based on those contracts.[695]

The fact that 2010 SCCs do not cover transfers from EEA processors to non-EEA processors is particularly problematic especially in the cloud environment. Solution a., in particular, would require EEA controllers to sign contracts with the non-EEA sub-processors engaged by their EEA processors (e.g., their cloud provider). However, this may lead to an excessive and unnecessary multiplication of the contracts that would need to be signed: if an EEA cloud provider (i.e., processor) has 4 non-EEA data centres (i.e., sub-processors) and 2.500 EEA customers (i.e., controllers), and the EEA customers decide to frame the transfer to the non-EEA data centres by means of SCCs, 10.000 SCCs will need be signed since every single EEA data controller would need to enter into SCCs with the 4 non-EEA sub-processors and 2.500 customers x 4 = 10.000.[696] Solution b. may be equally impractical since the inclusion in the service provider agreement of a mandate by the EEA controller to the EEA processor to enter into SCCs with the non-EEA processor would merely "transfer this workload on the Cloud provider".[697]

In 2009, the A29WP acknowledged the need to find a legal solution for framing international transfers from EEA processors to non-EEA processors and it "urge[d] the Commission to develop promptly a new separate and specific legal instrument that allows international sub processing by processors established in the Union to sub processors in a third country".[698] In 2014, the A29WP drafted a new set of contractual clauses for transfers from EEA processors to non-EEA processors.[699] However, these contractual clauses have not been approved by the European Commission so they do

[695] Ibid., 4–5.

[696] Emmanuelle Bartoli, *Data Transfers in the Cloud: Discussion Paper for the Commission's Expert Group on Cloud Computing Contracts*, 2014, 8, accessed August 3, 2018, https://docplayer.net/4162422-Data-transfers-in-the-cloud.html.

[697] Ibid.

[698] Article 29 Data Protection Working Party, *Opinion 3/2009 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC (Data Controller to Data Processor) (WP161)*, 2009, 3, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp161_en.pdf.

[699] Article 29 Data Protection Working Party, *Working Document 01/2014 on Draft Ad Hoc Contractual Clauses "EU Data Processor to Non-EU Sub-Processor" (WP214)*, 2014, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf.

not represent a new set of model clauses.[700] To remedy this situation, the GDPR recognizes the possibility to establish SCCs between EEA processors and non-EEA processors, although a new template that covers this type of transfer is yet to be developed. Article 46(3)(a), indeed, provides that appropriate safeguards may be provided for by "contractual clauses *between* the controller or *processor and* the controller, *processor* or the recipient of the personal data in the third country or international organisation".[701]

The difficulties that customers/controllers and cloud providers/processors may encounter when both EEA processors and non-EEA sub-processors are involved in the "supply chain" is representative of the limitations from which SCCs suffer when multiple (sub)processors situated in multiple locations are involved (as, after all, it is often the case in modern global transactions). SCCs seem, in fact, to be more suited for simple point-to-point transfers from identified data exporters to identified data importers: "SCCs are impractical for modern outsourcing transactions, like cloud, that typically involve globally provided services with dynamic data flows and chains of multiple providers and subproviders, datacentres and countries".[702] The difficulties that several companies encounter when trying to regulate "complex business arrangements"[703] by means of SCCs have been voiced, for instance, by Rackspace (2009) in its Consultation Paper on the Legal Framework for the Fundamental Right to Protection of Personal Data to the European Commission: "[w]hile the Standard Contractual Clauses work well for simple data transfers, they are not easy to apply for complex transfers through multiple service providers across global borders in the context of emerging

[700] Ibid., 2.

[701] Article 46(3)(a) GDPR. See also Recital 168 which refers to "standard contractual clauses between controllers and processors and *between processors*" (italics mine).

[702] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 194. See also, Hogan Lovells, *International Data Transfers. Considering Your Options*; US Chamber of Commerce and Hunton & Williams, *Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity*, 2014, 20, accessed August 7, 2018, https://www.uschamber.com/sites/default/files/documents/files/021384_BusinessWOBorders_final.pdf.

[703] Rackspace, *Consultation Paper on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2.

new IT technologies such as Cloud Computing".[704] When multiple parties are involved in the processing activities, even determining who should be party to SCCs is sometimes challenging.[705]

Microsoft participated to the same consultation where it reiterated that SCCs "are of limited utility because these provisions are difficult to use in organisations with many subsidiaries".[706] The need to extend the applicability of SCCs to multi-party contexts was also expressed by Orange/France Telecom Group.[707] To make things worse, the data importer may even refuse to undertake onerous SCCs obligations especially when the data importer is, for example, a large cloud provider (i.e., processor) while the data exporter a small company (i.e., controller). The implementation of SCCs in the cloud may hence be impractical considering large cloud providers' negotiating power.[708] In the light of the above, SCCs could be improved by making their structure more flexible and adaptable so as to capture the complexity of modern data processing operations "with multiparty, multijurisdictional and multilateral sharing of data".[709] SCCs should hence be revised so as to allow the signing by multiple parties.

A further difficulty derives from the fact that SCCs, as any other contract, need to be signed by two different legal entities. This makes SCCs unavailable when data controllers decide to move their data within the same organization for example by using their own third-country data centres. In a similar scenario, in order to avail itself of SCCs, the data controller would hence need to take the

---

[704] Ibid., 7.

[705] Ibid., 7–11.

[706] Microsoft Corporation, *Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 4.

[707] Orange/France Telecom Group, *Contribution to the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009, 3, accessed August 6, 2018, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/orange_en.pdf.

[708] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 200–201. The possibility that the data importer refuses to enter into SCCs with the data exporter is also acknowledged by the EDPB in its *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, adopted on 25 May 2018, where the EDPB noted that there may be cases "where the data importer has expressly refused to enter into a data transfer contract on the basis of standard data protection clauses" (p.15).

[709] Centre for Information Policy Leadership, *Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR*, 2019, 4, accessed December 9, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_paper_on_key_issues_relating_to_standard_contractual_clauses_for_international_transfers_and_the_way_forward_for_new_standard_contractual_clauses_under_the_gdpr.pdf.

additional (and artificial) step of establishing a separate legal entity that will operate the third-country data centres.[710] In the light of this, it can be concluded that although the abolition of mandatory pre-authorizations from DPAs may reduce the administrative burdens and related costs that under the DPD were affecting the recourse to SCCs, many other structural problems will be inherited by any new form of SCCs that may be adopted under the GDPR.[711]

Moreover, the same concerns about access to data for surveillance and/or enforcement purposes that have been expressed with reference to the Safe Harbour and the Privacy Shield frameworks can be extended to SCCs. The sets of SCCs approved by the European Commission deal with the risk that the legal framework to which the data importer is subject may prevent the data importer from complying with the provisions established under SCCs. Precisely, under 2001 SCCs, and similarly under 2004 SCCs[712] and 2010 SCCs,[713] the data importer is required to agree and warrant:

> that he has no reason to believe that the *legislation* applicable to him *prevents him from fulfilling his obligations under the contract* and that in the event of a change in that legislation which is likely to have a substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the data exporter and to the supervisory authority where the data exporter is established, in which case the data exporter is entitled to *suspend the transfer* of data and/or *terminate the contract*.[714]

In commenting on these provisions in the aftermath of the Snowden revelations, the A29WP noted that "considering [the Snowden's] revelations on the US surveillance programmes, there could be grounds for considering that the US legislation prevents the importer from fulfilling his obligations

---

[710] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 193.

[711] Ibid., 195.

[712] Under clause II(c), 2004 SCCs, the data importer warrants and undertakes that "[i]t has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws".

[713] Under Clause 5(b), 2010 SCCs, the data importer agrees and warrants "that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is *entitled to suspend the transfer of data and/or terminate the contract*" (italics mine). Moreover, under Clause 5(d)(i) 2010 SCCs, the data importer is required to inform the data exporter about "any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation".

[714] Clause 5(a), 2001 SCCs (italics mine).

under the contract and that the exporter could suspend the transfer of data/or terminate the contract".[715] It is however up to the non-EEA data exporters to establish whether transfers should continue.[716]

At the same time, 2010 SCCs allow for derogations to the contractual clauses when those derogations are necessary to meet mandatory requirements imposed by the legislation to which the non-EEA processor is subject that do *not* go beyond what is necessary in a democratic society:[717]

> [m]andatory *requirements* of the national legislation applicable to the data importer which do *not go beyond what is necessary in a democratic society* on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences ... *are not in contradiction* with the *standard contractual clauses*.[718]

Appendix 2 to 2001 SCCs contains the same principle where it is established that the data protection principles that the non-EEA data controllers shall follow when processing the transferred data "shall apply subject to the mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society".[719]

As a safeguard against the "problem of overriding law" (and against violations of the EU data protection principles more broadly), DPAs retain the power to prohibit or suspend the flow of data[720]

---

[715] Article 29 Data Protection Working Party, *WP228*, 42-43 (paragraph 5.2.2).

[716] Ibid., 43 (paragraph 5.2.2).

[717] The A29WP stressed that the exceptions included in SCCs, as well as in other data transfer mechanisms, "are limited in scope and should be interpreted restrictively (i.e. to be used in specific cases and for specific investigations). Since the adequacy instruments are primarily intended to offer protection to personal data originating in the EU, they should never be implemented to the detriment of the level of protection guaranteed by EU rules and instruments governing transfers" (Article 29 Data Protection Working Party, *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes (WP215)*, 2014, 7, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.)

[718] Fn.1 to Clause 5, 2010 SCCs (italics mine).

[719] Data protection principles "shall apply subject to the mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others". Appendix 2, 2001 SCCs.

[720] See Article 4 of Commission decisions 2001/497/EC and 2010/87/EU as amended by European Commission, *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 344/100, 2016). Commission Implementing Decision (EU) 2016/2297 amended Article 4 of Commission decision 2001/497/EC and Article 4 of Commission decision 2010/87/EU since the said articles posed some restrictive conditions under which DPAs could exercise their power to suspend the transfer of data. These limitations were comparable to the limitations on

when they determine "that the transfer is carried out in violation of EU or national data protection law, such as, for instance, when the data importer does not respect the standard contractual clauses".[721] Data exporters also retain control over the transferred data since they have the contractual right to suspend the transfer and/or to terminate the contract.[722] Such control is made effective by the several cooperation and audit obligations that SCCs impose on the data importer.[723] Despite these safeguards, SCCs are powerless when confronted with a generalised access on the part of public authorities[724] since contractual arrangements between two private parties are obviously incapable of putting any legal constraints on the intelligence activities of a third country.[725] Moreover, as noted by Hon (2017), any contractual prohibition to disclose data beyond what is necessary in a democratic society "would simply put importers in the impossible position of having to break laws [that require the data importer to disclose data] – or contracts [that requires the data importer not to disclose data beyond what is necessary in a democratic society] ... such conflicts cannot be resolved through contract".[726]

In addition, just like the Privacy Shield is currently facing invalidation risks, the validity of SCCs, in particular of 2010 SCCs for controller-processor transfers adopted with Commission decision 2010/87/EU, has been put into question. Indeed, on 12 April 2018, the Irish High Court

---

DPAs' powers laid out under Article 3(1) first subparagraph of the Safe Harbour decision which was declared invalid by the ECJ in *Schrems*.

[721] Recital 5, Commission Implementing Decision (EU) 2016/2297.

[722] Clause 5(a) 2001 SCCs; Clause VI(a) 2004 SCCs; Clause 5(a) and (b) 2010 SCCs.

[723] Among others, clause 5(d) 2001 SCCs prescribes that, at the request of the data exporter, the data importer shall submit "its data processing facilities for audit which shall be carried out by the data exporter or an inspection body ... where applicable, in agreement with the supervisory authority". Similarly, under clause II(g) 2004 SCCs, "[u]pon reasonable request of the data exporter, [the data importer] will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours ...". See also clause 5(f) 2010 SCCs under which the "data importer agrees and warrants: ... at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority".

[724] Linklaters, "The European Court of Justice to Rule on the Validity of Standard Contractual Clauses," last modified June 1, 2016, accessed August 6, 2018, https://www.linklaters.com/en/insights/publications/2016/june/the-european-court-of-justice-to-rule-on-the-validity-of-standard-contractual-clauses.

[725] Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," 907–908.

[726] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 197.

decided to bring to the attention of the ECJ several questions about the adequacy of 2010 SCCs in protecting personal data, and hence about the validity of Commission decision 2010/87/EU.[727] The case arose from a complaint by Maximillian Schrems who reformulated his complaint to the Irish DPA after the ECJ's decision in *Schrems* that led to the invalidation of the Safe Harbour. To overcome such invalidation, in fact, Facebook Inc., as many other companies, switched to SCCs in order to continue the flow of data from the EEA to the US. However, Schrems contested this extensive resort to SCCs considering that "there is no judicial remedy which would allow the data subject to take appropriate action to protect his personal data rights" and that "his personal data controlled by Facebook and processed by Facebook Inc. is at the very least 'made available' to US government authorities under various known and unknown legal provisions and spy programmes such as the 'PRISM' programme ...".[728] Schrems hence maintained that "Facebook cannot rely upon SCC Decision 'in the given situation of factual 'mass surveillance' and applicable US law that violate Article 7 [Right to respect for private and family life], 8 [Right to protection of personal data], and 47' [Right to an effective remedy and to a fair trial] of the Charter and the Irish Constitution".[729]

Several questions were referred by the Irish High Court to the ECJ. Among others, the Irish High Court asked whether EU law applies in cases where personal data are transferred via 2010 SCCs from the EU to third countries for commercial purposes and data are further processed for national security and/or law enforcement reasons notwithstanding the provisions under Article 4(2) of the Treaty on European Union (TEU) and Article 3(2) DPD. Indeed, Article 3(2) DPD provides that the Directive does "not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law" and national security is one of those fields pursuant to Article

[727] Request for a preliminary ruling, Article 267 TFEU, The High Court Commercial, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, http://www.europe-v-facebook.org/sh2/ref.pdf. The reference for a preliminary ruling was received by the Court of Justice on 9 May 2018: Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, Case C-311/18.

[728] Request for a preliminary ruling, Article 267 TFEU, The High Court Commercial, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, paragraph 17, http://www.europe-v-facebook.org/sh2/ref.pdf.

[729] Ibid., paragraph 18.

4(2) TEU which provides that "national security remains the sole responsibility of each Member State".[730] The Court also asked whether in determining whether the transfer of data to a third country by means of SCCs has caused a violation of the rights of an individual, the relevant "comparator" should be (a) the Charter, TEU, TFEU, the DPD, the European Convention on Human Rights or any other provisions of EU law, or (b) the national laws of one or more Member States.[731]

Moreover, the Court asked whether the fact that SCCs only apply to data exporters and data importers "and do not bind the national authorities of a third country who may require the data importer to make available to its security services for further processing the personal data transferred pursuant to the clauses provided for in the SCC Decision preclude the clauses from adducing adequate safeguards as envisaged by Article 26(2) of the Directive".[732] In the event that a "third country data importer is subject to surveillance laws that in the view of the DPA conflict" with the provisions under SCCs, the Court also asked whether national DPAs are required to exercise their power to suspend the flow of data, or if the exercise of that power is limited to exceptional cases, or if DPAs can use their own discretion not to suspend the flow of data.[733]

In addition, considering the findings of the European Commission in the Privacy Shield decision about the adequacy of the level of protection granted by the US, the Court asked whether that finding is binding for national data protection authorities and national courts and, if it is not, what relevance should the Privacy Shield decision have in assessing whether SCCs provide adequate safeguards.[734] As a logical conclusion of all these questions, the final question referred to the ECJ is whether Commission decision 2010/87/EU is in violation of Article 7, 8 and/or 47 of the Charter and should hence be declared invalid.[735]

[730] Ibid., question 1.
[731] Ibid., question 2.
[732] Ibid., question 7.
[733] Ibid., question 8.
[734] Ibid., question 9.
[735] Ibid., question 11.

The first hearing on the case before the ECJ took place on 9 July 2019. Some important statements were made by the EDPB in its oral pleading.[736] In particular, the EDPB noted that when SCCs are implemented, it is not up to the European Commission to assess whether the access by public authorities in a third country is consistent with the level of protection required by the EU. Rather, it is the responsibility of the EEA data exporter to make this assessment before entering into SCCs with a non-EEA data importer. Moreover, national DPAs retain the power to suspend the transfer of data if they conclude that the international transfer undermines the level of protection guaranteed within the EU. At the same time, the EDPB recalled that such an assessment is made on a case-by-case basis since DPAs do not have the power to pose a general ban to the transfer of data to a specific third country.[737]

Moreover, the EDPB stressed that, no matter which data transfer mechanism is implemented, "the continuity of the protection afforded under EU laws needs to be ensured, also during the stage of transit to a third country". This entails that when assessing the adequacy of the level of protection of a third country's legal order, the European Commission should also examine the laws and practices that give its public authorities the possibility to intercept data outside its borders. At the same time, this analysis should be limited to the laws and practices that apply in the country where the recipient is located and should hence not extend to the laws of any another country which may allow for surveillance while data are on their way to the recipient's country.[738] The EDPB also stressed that more specific safeguards should be implemented so as to limit the US programs for surveillance and expressed doubts about the capability of the Ombudsperson mechanism to offset the deficiencies of the judicial remedies before the US courts.[739]

[736] European Data Protection Board, *Oral Pleading before the Court of Justice of the EU Case C-311/18 (Facebook Ireland and Schrems)*, 2019, accessed December 8, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/20190709edpbpleadingschremsii_-_for_publication.pdf.

[737] Ibid., 1–2.

[738] Ibid., 2.

[739] Ibid., 4–5.

Certainly, organizations that rely on SCCs have been – at least temporarily – comforted by the opinion delivered on 19 December 2019 by Advocate General Saugmandsgaard Øe.[740] Indeed, in the view of the Advocate General, Commission decision 2010/87/EU is valid. In reaching this conclusion, he stressed that since contractual safeguards have been designed precisely for ensuring the continuity of protection were the safeguards afforded in the third country of destination are inadequate, the validity of Commission decision on SCCs cannot depend of the level of protection guaranteed in the third country to which data are transferred by means of those contractual clauses. Rather, the "validity of such a decision depends only on the soundness of the safeguards which those clauses provide in order to compensate for any inadequacy of the protection afforded in the third country of destination".[741] And according the Advocate General, the safeguards provided by the clauses in question are, indeed, sound since they include mechanisms for suspending or prohibiting the transfer of data when the clauses have been breached or cannot be complied with.

As noted by the Advocate General, the SCCs take into account situations where "the prevailing legal context in the third country of destination ... make the obligations set out in those clauses impossible to implement".[742] In those situations,

> the contractual mechanism set out in Article 46(2)(c) of the GDPR is based on responsibility being placed on the exporter and, in the alternative, the supervisory authorities. It is on a case-by-case basis, for each specific transfer, that the controller or, failing that, the supervisory authority will examine whether the law of the third country of destination constitutes an obstacle to the implementation of the standard clauses and, therefore, to an adequate protection of the transferred data, so that the transfers must be prohibited or suspended.[743]

To sum up, according to the Advocate General, the validity of the Commission decision relies on the obligation placed on the controller, or when the controller fails, on the competent DPA to suspend or prohibit the transfer when the clauses cannot be honoured. If the ECJ follows the same approach, the approximately 88% of companies that transfer data to third countries by means of SCCs[744] could

[740] Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, *Facebook Ireland and Schrems*, Case C-311/18.
[741] Ibid., paragraph 124.
[742] Ibid., paragraph 125.
[743] Ibid., paragraph 126.
[744] International Association of Privacy Professionals and Ernst & Young, *Annual Privacy Governance Report 2019*, 2019, 77, accessed January 2, 2020, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.

continue to rely on these clauses. Otherwise, EU businesses would need to resort to other data transfer mechanisms or, as a more drastic solution, "re-engineer their systems" by processing personal data exclusively by using EU data centres "which could raise other types of issues such as financial and environmental ones but also in terms of protectionism".[745]

5.5.2. Binding Corporate Rules

Transfer of personal data to third countries can also take place by means of Binding Corporate Rules. BCRs are internal rules, like codes of conduct, that allow international data transfers between the members of a group of undertakings, or of a group of enterprises engaged in a joint economic activity.[746] BCRs were not explicitly included in the 1995 Directive. However, in WP74 (2003),[747] the A29WP decided to exploit the "broad margin of manoeuvre" offered by Article 26(2) DPD and concluded that "there should not be any reason to exclude" the possibility to rely on internal codes of conduct "[i]n so far as a unilateral undertaking is able to deploy real and ensured legal effects, in particular as regards the effective protection of data subjects after the transfer and as regards the possible intervention of national supervisory authorities or other authorities".[748] In WP74, the A29WP hence concluded that Binding Corporate Rules[749] could be considered as an additional tool on which companies can rely when the recourse to the existing transfer mechanisms is particularly problematic.[750] The GDPR formalizes the possibility to frame international transfer by using BCRs

[745] Linklaters, "The European Court of Justice to Rule on the Validity of Standard Contractual Clauses." "... [A] number of questions concerning the validity of the Model Clauses have been referred to the Court of Justice of the European Union. Organizations that rely on Model Clauses should therefore pay careful attention as the playing field may change in the future. In this quickly changing environment, organizations should prepare for alternative solutions or be ready to adapt if needed...". Nathalie McNabb and Soeren Klaebel Clemmensen, "GDPR Update: The Future of International Data Transfers," *Deloitte*, accessed January 17, 2019, https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-future-of-international-data-transfers.html.

[746] Article 47 GDPR; Recital 110 GDPR.

[747] Article 29 Data Protection Working Party, *WP74*.

[748] Ibid., 5.

[749] "[B]inding ... because only with such a character may any clauses be regarded as 'sufficient safeguards' within the meaning of Article 26 (2)" and "corporate in the sense that they consist of the rules in place in multinational companies, usually set up under the responsibility of the headquarters". Ibid., 8.

[750] Ibid., 6.

and extends this possibility to enterprises which are not part of the same group but which are engaged in joint economic activities.

The A29WP has issued guidelines about the requirements that should be included in both BCRs for controllers (BCR-C) and BCRs for processors (BCR-P). BCR-C can be used to transfer personal data from EEA controllers to non-EEA controllers or non-EEA processors that are part of the same group of the EEA controller: "[h]ence the obligations set out in the BCR-C apply in relation to entities within the same group acting as controllers and to entities acting as 'internal' processors".[751] On the other hand, BCR-P apply to the transfer of data between processors/sub-processors of the same group when those data have been received by an EEA controller which is not part of the group:[752] "[h]ence the obligations set out in the BCR-P apply in relation to third party personal data that are processed by a member of the group as a processor according to the instructions from a non-group controller".[753] BCR-P have proved particularly useful considering the limitations from which, as seen above, SCCs suffer when it comes to massive multi-party transfers from EEA processors to non-EEA (sub)processors.[754] The requirements for BCR-C were first set out by the A29WP in WP153,[755] while the requirements for BCR-P were first set forth in WP195.[756] The A29WP has then updated the requirements for both BCR-C (in WP256 rev.01) and BCR-P (in WP257 rev.01) in order to take into account the requirements under Article 47(2) GDPR that lists a minimum set of elements that should be included in BCRs.

---

[751] Article 29 Data Protection Working Party, *Working Document Setting up a Table with the Elements and Principles to Be Found in Binding Corporate Rules (WP256 Rev.01)*, 2018, 2, accessed December 15, 2019, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

[752] Ibid.

[753] Article 29 Data Protection Working Party, *Working Document Setting up a Table with the Elements and Principles to Be Found in Processor Binding Corporate Rules (WP257 Rev.01)*, 2018, 2, accessed December 15, 2019, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

[754] Article 29 Data Protection Working Party, *Explanatory Document on the Processor Binding Corporate Rules (WP204 Rev.01)*, 2015, 5, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf.

[755] Article 29 Data Protection Working Party, *Working Document Setting up a Table with the Elements and Principles to Be Found in Binding Corporate Rules (WP153)*, 2008, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf.

[756] Article 29 Data Protection Working Party, *Working Document 02/2012 Setting up a Table with the Elements and Principles to Be Found in Processor Binding Corporate Rules (WP195)*, 2012, accessed December 15, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

BCRs have so far proved to be an efficient tool for framing international data transfers. BCRs allow, in fact, to carry out multiple transfers between multiple companies of the same group by means of one single instrument: "[m]ore than a set of legal rules, BCR can serve the establishment of an effective global policy, of an 'internal standard' for personal data protection within the group. Indeed, they apply indiscriminately to the whole corporate group, regardless of the establishment of the subsidiaries or of data subjects' citizenship".[757]

The main problem affecting BCRs is the length and the complexity of the procedure for their approval by the competent DPA(s). The approval of BCRs may, in fact, take months or years to complete, and some companies even have some specialized staff in charge of dealing with BCRs.[758] The administrative burdens and costs that the implementation of BCRs require may hence make the recourse to BCRs practically impossible for SMEs. The EDPB (2018) itself has recognised that BCRs "may often not be a feasible option" when the data exporter is a small or medium-sized company.[759] Taking into account these difficulties, the GDPR prescribes that once BCRs have been approved by the competent BCR Lead Supervisory Authority, the approved BCRs will provide for appropriate safeguards without requiring any specific authorisation from the other DPAs concerned.[760] However, according to Hon (2017), the fact that the BCRs approval process will now trigger the consistency mechanism pursuant to Articles 63 GDPR ff.[761] may "increase complexity and delays (and therefore affect affordability for SMEs), or even result in rejection of BCR applications".[762]

---

[757] Olivier Proust and Emmanuelle Bartoli, "Binding Corporate Rules: A Global Solution for International Data Transfers," *International Data Privacy Law* 2, no. 1 (2012): 36.

[758] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 206.

[759] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 2018, 15n40, accessed December 15, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf. See also, McNabb and Klaebel Clemmensen, "GDPR Update: The Future of International Data Transfers."

[760] Article 46(2)(b) GDPR. On the procedure for the approval of BCRs, see Article 29 Data Protection Working Party, *Working Document Setting Forth a Co-Operation Procedure for the Approval of "Binding Corporate Rules" for Controllers and Processors under the GDPR (WP263 Rev.01)*, 2018, accessed December 15, 2019, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056.

[761] Article 47(1) GDPR prescribes that "[t]he competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, ...".

[762] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 209.

Moreover, the fact that BCRs only apply to intra-group transfers severely affects the potential utility of this transfer mechanism. Indeed, this inherent limitation make BCRs particularly ill-suited for the cloud computing environment that is populated by layered services where several third-party processors/sub-processors are involved.[763] In addressing this limitation, the GDPR now extends the applicability of BCRs to "group[s] of enterprises engaged in a joint economic activity".[764] However, the definition of "group[s] of enterprises engaged in a joint economic activity" – and how that differs from "group of undertakings" defined in Article 4(19) GDPR[765] – is unclear. Considering the length of the BCR approval process, it can be presumed that the enterprises involved will tend to be bound by a close and long-term relationship for them to wish to undertake the lengthy and burdensome process of BCR approval. Again, this would limit the practical utility of BCRs for the cloud where the relationship between the parties involved is often fluid and changeable.[766]

Moreover, just like the Privacy Shield and SCCs, BCRs may be exploited to allow the transfer of data from the private to the public sector and, in particular, to law enforcement and national security authorities. This is why, both BCR-C and BCR-P shall include detailed provisions about the commitments that BCR members shall undertake in the event that the legislation to which they are subject prevents them from complying with BCRs. BCR-C, in particular, shall include

> [a] clear commitment that where a BCR member has reasons to believe that the *legislation* applicable to him *prevents the company from fulfilling its obligations under the BCRs* or has substantial *effect on the guarantees provided by the rules*, he will promptly inform the EU headquarters or the EU BCR member with delegated data protection responsibilities and the other relevant Privacy Officer/Function (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).[767]

[763] Ibid., 207–208.

[764] Article 47 GDPR; Recital 110 GDPR.

[765] Article 4(19) GDPR defines "group of undertakings" as "a controlling undertaking and its controlled undertakings".

[766] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 209. The A29WP also noted that for "loose conglomerates, binding corporate rules are very unlikely to be a suitable tool. The diversity between their members and the broad scope of the processing activities involved would make it very difficult (if not impossible) to meet the requirements" for approval of BCRs (WP74, 9).

[767] Criterion 6.3 for approval of BCRs (italics mine), Article 29 Data Protection Working Party, *WP256 Rev.01*.

The same problem should be reported to the competent DPA, which should also be informed of "any legally binding request for disclosure of the personal data by a law enforcement authority or state security body", unless the confidentiality of the investigation prohibits such a communication. In this latter case, the BCR member subject to the disclosure request shall "use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible". If, despite its best effort, the BCR member concerned is still not in the position to inform the competent DPA, it shall commit to annually provide the DPA with general information about the requests it has received (e.g., the number of requests received, the types of data involved). "In any case, the BCRs must state that transfers of personal data by a BCR member of the group to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society".[768]

In the same vein, BCR-P shall include a clear commitment that "where a BCR member has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the controller or its obligations under the BCRs" or under the service agreement, it will notify the controller, which is entitled to suspend the transfer of data or terminate the contract, "the EU headquarter processor or EU member with delegated data protection responsibilities or the other relevant Privacy Officer/function", and the DPA competent for the controller and the DPA competent for the processor. The controller, the competent DPA for the controller and the competent DPA for the processor shall also be informed of any legally binding requests for disclosure by law enforcement authorities or security bodies, unless otherwise prohibited.[769] Moreover, and as a general rule, it should be recalled that transfer of personal data to law enforcement authorities and/or state security bodies shall always be carried out on the basis of a legal ground since the commitments that BCRs must include in the event of requests for disclosures

[768] Criterion 6.3 for approval of BCRs, Ibid.
[769] Criterion for approval of BCRs n. 6.3, Article 29 Data Protection Working Party, *WP257 Rev.01*.

only impose information requirements on the non-EEA BCR member but do not legitimise *per se* the transfer.[770]

Despite the provisions above, the adequacy of BCRs in providing appropriate safeguards seem to be at stake. Indeed, in its opinion on the EU-U.S. Privacy Shield draft adequacy decision (2016) where, as seen above (5.4.4.), the EDPS has expressed several concerns about the adequacy of the Privacy Shield in protecting personal data, the EDPS noted that many of the considerations that it expressed with reference to the Privacy Shield also indirectly apply to other transfer mechanisms like BCRs and SCCs.[771] Similarly, in its Statement on the decision of the European Commission on the EU-U.S. Privacy Shield (2016), the A29WP noted that the "first joint review regarding access by U.S. public authorities to data transferred under the Privacy Shield may also impact transfer tools such as Binding Corporate Rules and Standard Contractual Clauses"[772] and, as seen above (5.4.4.), in its first annual joint review, the A29WP has identified several unresolved issues with reference to the access by public authorities to personal data transferred from the EU to the US.[773]

5.5.3. Other Appropriate Safeguards: Ad Hoc Contracts, Data Transfer in the Public Sector, Codes of Conduct and Certifications

The GDPR also allows controllers/processors to transfer data to third countries on the basis of ad hoc contractual clauses subject to the approval of the competent supervisory authority.[774] The possibility to resort to ad hoc contracts was also permitted under the 1995 Directive. Article 46(4) of the GDPR, however, now prescribes that supervisory authorities shall apply the consistency

[770] Article 29 Data Protection Working Party, *WP204 Rev.01*, 12.

[771] European Data Protection Supervisor, *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, 6.

[772] Article 29 Data Protection Working Party, *Statement on the Decision of the European Commission on the EU-U.S. Privacy Shield*, 2016, accessed December 15, 2019, 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.

[773] Article 29 Data Protection Working Party, *WP255*, 14–20.

[774] Article 46(3)(a) GDPR.

mechanism referred to in Article 63, which should be judged positively since it aims at guaranteeing a uniform regulatory approach across the EU.[775]

New legal bases for transfer have also been introduced in the public sector. Pursuant to Article 46(2)(a) GDPR, transfer of data may take place by virtue of "a legally binding and enforceable instrument" between public bodies without requiring any authorization from the competent DPA. The authorization by the competent DPA is instead required when appropriate safeguards are provided by means of "administrative arrangements between public authorities", such as memorandum of understanding, which are not legally binding.[776] These arrangements shall also include "enforceable and effective data subject rights".[777]

On 12 February 2019, the EDPB has adopted its first opinion on a draft Administrative Arrangement (AA) for cross-border data flow, precisely, on the draft Administrative Arrangement for the transfer of personal data between EEA and non-EEA Financial Supervisory Authorities.[778] Considering the guarantees set out under the AA and the commitments that EEA Financial Supervisory Authorities and their non-EEA counterparts would undertake by signing the AA,[779] the EDPB concluded that the arrangement in question ensures appropriate safeguards. The national DPAs may hence now authorize international data transfers based on this administrative arrangement. After having obtained such authorization, the EEA financial supervisory authorities will consequently be able to transfer data to third countries by entering into an administrative arrangement with their non-

[775] Gabel and Hickman, "Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation."

[776] Article 46(3)(b) and Recital 108 GDPR.

[777] Ibid. See also, 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 - Version 1.0*, 2020, accessed July 8, 2020, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v1.pdf.

[778] European Data Protection Board, *Opinion 4/2019 on the Draft Administrative Arrangement for the Transfer of Personal Data between European Economic Area ("EEA") Financial Supervisory Authorities and Non-EEA Financial Supervisory Authorities*, 2019, accessed December 10, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/2019-02-12-opinion_2019-4_art.60_esma_en.pdf. This opinion was issued pursuant to Article 64(3) GDPR.

[779] The draft AA contains definitions of GDPR concepts and data subject rights; the principle of purpose limitation and prohibition of any further use; the principle of data quality and proportionality; the principle of transparency; the principle of data retention; security and confidentiality measures; safeguards relating to data subject rights; restrictions on onward transfers; redress; oversight mechanism.

EEA counterparts.[780] The first authorization was given on 23 May 2019 by the Italian DPA (*Garante per la Protezione dei dati personali*) which, taking into account the positive opinion issued by the EDPB on the said agreement, authorized the Italian public Authority responsible for regulating the national financial market (*Commissione Nazionale per la Società e la Borsa*) to frame the transfer of personal data to non-EEA Authorities on the basis of the said agreement.[781]

Codes of conduct and certification mechanisms can also be used to frame international data transfer. A company that is not (directly) subject to the GDPR by virtue of Article 3 may, in fact, provide appropriate safeguards by adhering to a code of conduct pursuant to Article 40[782] or by receiving a certification pursuant to Article 42.[783] Both codes of conduct and certifications need to be complemented with "binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights".[784] This entails that the commitment to apply the appropriate safeguards embedded in codes of conduct and certification mechanisms need to be made legally binding by means of contractual solutions or other legal instruments in order for them to constitute a valid legal basis for transfer.

More specifically, under Article 40 GDPR, "[t]he Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises."[785] Codes of conduct may also be prepared by associations and other bodies representing categories of

---

[780] Emmanuel Ronco and Natalie Farmer, "EDPB Issues First Opinion on Administrative Arrangements Under the GDPR for Cross-Border Data Flows Between EU and Non-EU Securities Agencies," *Cleary Cybersecurity and Privacy Watch*, last modified March 15, 2019, accessed May 1, 2019, https://www.clearycyberwatch.com/2019/03/edpb-issues-first-opinion-on-administrative-arrangements-under-the-gdpr-for-cross-border-data-flows-between-eu-and-non-eu-securities-agencies/.

[781] Garante per la Protezione dei dati personali, *Authorisation to CONSOB for Entering into an Administrative Agreeement for the Transfer of Personal Data between the EEA Financial Supervisory Authorities and the Non-EEA Financial Supervisory Authorities (9119857)*, 2019, accessed December 15, 2019, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9119857. The administrative agreement is available at the following link: http://www.consob.it/documents/46180/46181/accordo-privacy-2019.pdf/b2471a58-d362-4c04-9d8b-c84dff7b6b52.

[782] Article 40(3) GDPR.

[783] Article 42(2) GDPR.

[784] Article 46(2)(e) and Article 46(2)(f) GDPR.

[785] Article 40(1) GDPR.

controllers and processors.[786] Codes of conduct hence mainly aim to meet the needs of specific sectors which constitutes both an advantage, since these codes allow to make controllers/processors' obligations more tailored to the specificities of the sectors in which they are involved, and, at the same time, a limitation of codes of conduct as transfer mechanisms, since "companies with multi-sectoral activities" may face "substantial difficulty to adhere to multiple Codes of Conduct".[787] The EDPB has highlighted the potentials of codes of conduct not only as an instrument for enabling data transfers but also as a medium for promoting and spreading internationally the EU standards for data protection:

> ... approved codes of this nature may result in the promotion and cultivation of the level of protection which the GDPR provides to the wider international community while also permitting sustainable legally compliant international transfers of personal data. They may also serve as a mechanism which further develops and fosters data subject trust and confidence in the processing of data outside of the European Economic Area.[788]

However, specific guidelines on codes of conduct as a tool for international data transfer has not been published yet.[789]

Article 42 GDPR is instead devoted to data protection certifications, seals and marks. Pursuant to Article 42(1) GDPR, the use of similar mechanisms shall be encouraged by the Member States, supervisory authorities, the EDPB and the Commission "for the purpose of demonstrating compliance" with the GDPR in the course of the processing activities conducted by controllers and processors.[790] Besides helping controllers and processors demonstrating compliance with the GDPR, Article 42(2) GDPR provides that data protection certifications, seals or marks "may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of

[786] Article 40(2) GDPR.

[787] Irene Kamara et al., *Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679* (Brussels: European Commission - DG Justice & Consumers, 2019), 184, accessed May 1, 2019, https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_final.pdf.

[788] European Data Protection Board, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - Version 2.0*, 2019, 10 (paragraph 17), accessed December 15, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf.

[789] "Guidance on codes of conduct as a tool for transfers of data as per Article 40(3) of the GDPR will be considered in separate guidelines to be issued by the EDPB". Ibid., 6 (paragraph 5).

[790] Article 42(1) GDPR.

personal data transfers to third countries or international organisations" under Article 46(2)(f) GDPR.[791] In other words, on the one hand, under Article 42(1) GDPR, the applicant *is* subject to the GDPR and the certification mechanism aims to demonstrate that the controller/processor complies with the GDPR; on the other hand, under Article 42(2) GDPR, the applicant *is not* subject to the GDPR and the certification mechanism aims to show that the *non-EEA* controller/processor provides appropriate safeguards for data transfer.[792]

It is hence clear that, unlike SCCs and BCRs, the applicant for certification is not the EEA data controller/processor but it is the *non-EEA* controller/processor that wishes to have its processing activities certified pursuant to Article 42(2) in order to receive data from the EU.[793] A non-EEA data importer may hence decide to apply for a certification mechanism even in the absence of a pre-existing relationship with an EEA data exporter. This may significantly boost possibilities for cross-border data transfers since "data exporters may be assisted in their selection of controllers or processors who have already been audited by an independent accredited certification body and were granted certification". At the same time, by adhering to a certification mechanism, data importers can "signal" to EEA data exporters their reliability and so ease their entrance in the EU market.[794] Moreover, while codes of conduct are mainly meant to offer an efficient data transfer tool for companies in a specific sector, certification mechanisms can be "sector-neutral" which makes it a more flexible tool.[795]

The object of certification pursuant to Article 42(2) GDPR is the processing operation or the set of processing operations conducted by the non-EU applicant, whether data controller or data processor.[796] The EDPB has identified several certification criteria in its Guidelines on Articles 42(1) and 43 GDPR, which are all derived from the GDPR principles: the lawfulness of processing (Article

[791] Article 42(2) GDPR.
[792] Kamara et al., *Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679*, 175.
[793] Ibid., 176.
[794] Ibid., 182.
[795] Ibid., 184.
[796] Ibid., 176–177.

6); the principles of data processing (Article 5); the data subjects' rights (Articles 12-23); the obligation to notify data breaches (Article 33); data protection by design and by default (Article 25); whether a data protection impact assessment, pursuant to Article 35(7)(d) has been conducted; and the implementation of technical and organisational measures (Article 32).[797] However, specific criteria for the purpose of demonstrating the existence of appropriate safeguards pursuant to Article 42(2) are still missing.[798]

Moreover, just like codes of conduct, the enforceability of certifications pursuant to Article 42(2) GDPR is achieved by complementing the certification mechanism with "binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights".[799] Such commitments could translate into bilateral, multilateral contracts or in unilateral commitments or in international treaties between two or more States.[800] Such legally binding and enforceable commitments should also include third party beneficiary rights in order to guarantee a remedy to data subjects which have suffered harm from non-compliance with the certification mechanism.[801] Clarifications on the exact shape and content that these legally binding and enforceable commitments should take is however needed but, even in the absence of such clarifications, it can be assumed that the need to complement certification mechanisms with further commitments may represent an obstacle to the smooth transfer of data from EEA data exporters to certified non-EEA data importers (presumably, especially if such commitments would need to be included in multilateral contracts or would be created by means of treaties).

Interestingly, back in 2009, Rackspace suggested that a certification system should be implemented as a means to overcome the limitations of the existing EU data transfer rules:

> All [the] different instruments used for international data transfer could be *combined in one* solution, where businesses would be able to *certify* their handling of data worldwide ... A

[797] European Data Protection Board, *Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation - Version 3.0*, 2019, 15, accessed December 10, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf.

[798] Ibid., 28.

[799] Article 46(2)(f).

[800] Kamara et al., *Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679*, 197–204.

[801] Ibid., 208–209.

> workable solution for *global self-certification* would enable companies to *certify that adequate safeguards are in place* concerning its global data processing operations. A simple certification that would allow companies to certify that adequate safeguards are in place concerning their data processing operations *for intra-group data transfers*, as well as for *external data transfers* (where data is received for processing from a third party who uses its data processing services), could be a useful tool to be taken into consideration for future improvement of existing legal framework.[802]

Rackspace hence suggested that the various, yet often unworkable, data transfer mechanisms laid out under the EU data protection legislation could be replaced by one solution under which companies would be able to self-certify that their processing operations are subject to adequate safeguards.[803] Unlike the certification mechanism under Article 42(2), however, Rackspace has proposed a data transfer regime based on *self*-certification rather than on certification by third parties. Moreover, even BCRs resonate in the references made by Rackspace to the *global* data processing operations of the self-certified company and to the fact that the certification would cover their handling of data *worldwide*.

One of the most interesting suggestions advanced by Rackspace is the possibility to maintain a list – preferably *two* lists, one for processors and one for controllers – of the companies that are certified as providing adequate safeguards: the "EU authorities would maintain such list of companies that certified that they have adequate safeguards in place when processing personal data on a global level".[804] Thanks to this list, on the one hand, data exporters could easily identify reliable data importers that are certified as capable of processing data in compliance with EU data protection rules and, on the other, non-EU data importers could easily show their capacity to provide an adequate level of protection. Such system would be especially beneficial for non-EEA SMEs which aim to make themselves "visible" outside their jurisdiction in order to engage in international economic

[802] Rackspace, *Consultation Paper on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 11–12.

[803] "Any data controller that would need additional guarantees for personal data processing could set this out in a contract with its service provider without additional requirements on signing the Standard Contractual Clauses when such data is transferred to a service provider located in a country not considered to provide an adequate level of protection. When a company would not self-certify, applicable Standard Contractual Clauses would have to be signed in addition to a general data processing agreement". Ibid., 12.

[804] Ibid.

relations. In the light of the above, the inclusion of certified companies in specific lists, or better two lists, one for controllers and one for processors, should also be considered under Article 42(2) GDPR.

Overall, the possibility to resort to codes of conduct and certification mechanisms as (new) legal bases for transfer seems promising. Certainly, adhering to a code of conduct or earning a certification may still involve considerable administrative costs (and time) especially for SMEs.[805] For example, "certification may be a lengthy process, and the outcome may be negative for the applicant or corrective actions might need to be undertaken before the certification is granted".[806] However, these costs may be compensated by the possibility to easily identify controllers/processors not subject to the GDPR that provide appropriate safeguards, "for example, via screening for those adhering to a code or displaying a certification seal". Overall, this may facilitate international data transfer.[807] However, it is unclear at this stage how these new transfer mechanisms will develop in practice and how effective they will be in granting protection to transferred data.

5.6. Derogations

Pursuant to Article 49 GDPR, in the absence of an adequacy decision and in absence of appropriate safeguards, international transfer may take place only if some conditions are met. Derogations are at the bottom of the hierarchy after adequacy decisions and appropriate safeguards. This derives from the fact that derogations do not guarantee that the data subjects will continue to enjoy the same level of protection they are afforded in the European Union once data are transferred to third countries. Derogations, in fact, do not provide neither for adequate protection (pursuant to Article 45 GDPR) nor for appropriate safeguards (pursuant to Article 46 GDPR) and they are not subject to any prior authorization before transfer. Derogations are hence exceptions to the general rule that transfer shall only take place if the third country provides an adequate level of protection or

[805] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 212.

[806] Kamara et al., *Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679*, 193.

[807] Rita Heimes, "Top 10 Operational Impacts of the GDPR: Part 9 - Codes of Conduct and Certifications," *Iapp*, February 24, 2016, accessed January 17, 2019, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/.

if appropriate safeguards are adduced by the controller or processer and should hence be interpreted restrictively.[808]

Moreover, as an overarching condition, the EDBP stressed that a necessity test should be applied to the derogations under Article 49(1)(b), (c), (d), (e), (f). All these derogations, in fact, only apply if the data exporter deems the transfer *necessary* for achieving a specific purpose. Recital 111 GDPR also adds that transfer in relation to a contract (Article 49(1)(b), (c)) and the transfer in relation to a legal claim (Article 49(1)(e)) shall take place only if it is "occasional". Similarly, under Article 49(1) paragraph 2, transfer may take place if it "is necessary for the purposes of compelling legitimate interests pursued by the controller" and only if the transfer is "not repetitive". The terms "occasional" and "not repetitive" mean 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".[809] The EDPB also noted that even if the other derogations are not explicitly limited to occasional transfers, they will have to be interpreted in a way that preserves their nature of exception to the general rules set out under Articles 44-47. This entails that reliance on these "exceptional" grounds need to be restricted to specific situations.[810] The derogations under Article 49 will now be analysed in greater detail.

Article 49(1)(a): the data subject has explicitly consented to the proposed transfer. The general requirements of valid consent are prescribed under Article 4(11) and 7 GDPR.[811] Article 49(1)(a) prescribes some additional requirements for consent to be a valid legal basis for transfer: consent must be "explicit"[812] and, as a specification of the general requirement under Article 4(11) that consent must be "informed", Article 49(1)(a) adds that data subjects must have been "informed

[808] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 3–4.

[809] Ibid., 4.

[810] Ibid., 5.

[811] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679 (WP259 Rev.01)*, 2018, accessed December 15, 2019, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[812] Under Article 4(11) GDPR, consent shall be "freely given, specific, informed and unambiguous" but not explicit.

of the possible risks of such transfers ... due to the absence of an adequacy decision and appropriate safeguards".[813] The EDPB has also stressed that, as a general requirement of valid consent, it must be specific for the particular transfer(s) of data.[814]

Article 49(1)(b): the transfer 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 requests. The applicability of this (potentially fairly broad) derogation is limited by two criteria: the necessity criterion and the occasional criterion. This entails, on the one hand, that there has to be "a close and substantial connection between the data transfer and the purposes of the contract" and, on the other hand, that the transfer shall not be systematic and repeated.[815]

Article 49(1)(c): the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person. The interpretation of this derogation is similar to the one suggested under Article 49(1)(b): a close link shall be identified between the transfer of data and the contract concluded in the interest of the data subjects, and transfer must be occasional.[816]

Article 49(1)(d): the transfer is necessary for important reasons of public interest. This derogation only applies when the public interest invoked as a basis for transfer is recognized in the EU legal system or in the Member State law to which the data controller is subject.[817] As clarified by

---

[813] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 7. "The information provided to data subjects in order to obtain consent for the transfer of their personal data to third parties established in third countries should also specify all data recipients or categories of recipients, all countries to which the personal data are being transferred to, that the consent is the lawful ground for the transfer, and that the third country to which the data will be transferred does not provide for an adequate level of data protection based on a European Commission decision. In addition, as mentioned above, information has to be given as to the possible risks for the data subject arising from the absence of adequate protection in the third country and the absence of appropriate safeguards. Such notice, which could be standardized, should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country". Ibid., 8.

[814] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 7. The EDPB has clarified that consent can be regarded as a valid legal ground for transfer when the data subject has consented to the specific transfer "at the time when the transfer is envisaged". This entails that if the occurrence of data transfer is not foreseen at the time of the collection of data, the consent obtained by the EU data controller at the time of the data collection does not constitute a valid ground to enable the transfer to third countries but the data exporter will be required to obtain specific consent before that specific transfer or set of transfers.

[815] Ibid., 8–9.

[816] Ibid., 9–10.

[817] Article 49(4) GDPR.

the EDPB, "the derogation 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".[818] The fact that the EU or a Member State have entered into an international agreement with a third country under which both parties undertake international cooperation to pursue a specific objective may be an indicator of the existence and of the recognition of a specific public interest in the EU.[819] This derogation may be relied upon not only by public authorities but also by private entities. The applicability of this derogation is hence dependant on the nature of the interest pursued rather than on the private or public nature of the entity concerned.[820]

Article 49(1)(e): the transfer is necessary for the establishment, exercise or defence of legal claims. This derogation applies regardless of whether the transfer is necessary "in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies".[821] A wide range of activities seems to fall under this derogation such as criminal and administrative investigations, pre-trial discovery procedures, activities that are necessary for instituting a procedure in a third country. At the same time, some limitations to the applicability of this derogation have also been highlighted by the EDPB: the derogation shall not be invoked to justify the transfer of data on the basis of the mere possibility that legal claims may be brought in the future; the procedure in question must be grounded on a legal norm; a close link shall be identified between

[818] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 10.
[819] Ibid.
[820] Ibid., 11.
[821] Recital 111, GDPR.

the transfer of data and the "establishment, exercise or defence" of the legal claim (necessity criterion);[822] and the transfer shall not occur on a systematic basis (occasional criterion).[823]

Article 49(1)(f): the transfer is necessary in order to protect the vital interests of the data subject or of other persons. This derogation refers to situations where the law assumes that situations of medical emergencies outweigh data protection concerns, such as in the case where transfer of data is necessary in order to give an unconscious patient the required medical treatment, in order to make an essential diagnosis, or for the purpose of conducting rescue operations after natural disasters. This derogation only applies when the data subject concerned is physically (e.g., unconscious patients) or legally (e.g., minors) incapable of giving consent. Moreover, this derogation aims to protect the vital interests not only of the data subjects but also of other persons.[824]

Article 49(1)(g): the transfer is made from a public register. The register referred to in this Article must be intended to provide information to the public according to EU or Member State law. The register must be "open to consultation either by the public in general or by any person who can demonstrate a legitimate interest".[825] Examples include: "registers of companies, registers of associations, registers of criminal convictions, (land) title registers or public vehicle registers".[826] Moreover, transfer of data pursuant to Article 49(1)(g) shall not involve the entire set of data contained in the register and, "[w]here the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients".[827]

---

[822] "Whilst there may be a temptation for a data exporter to transfer all possibly relevant personal data in response to a request or for instituting legal procedures, this would not be in line with this derogation or with the GDPR more generally as this (in the principle of data minimization) emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 12. In order to limit the amount of transferred data, the EDPB also invites the data exporters to consider the possibility to resort to some technical solutions (as an alternative to legal solutions, and hence to legal bases for transfer). Sometimes, in fact, the transfer of *anonymized* data or *pseudonymized* data may be sufficient.

[823] Ibid.

[824] Ibid., 12–13.

[825] Article 49(1)(g) GDPR.

[826] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 14.

[827] Article 49(2) GDPR.

Article 49(1) paragraph 2: compelling legitimate interests. This derogation applies as a last resort where none of the other transfer tools is available (i.e., adequacy decisions, appropriate safeguards, and the derogations listed above). Moreover, the possibility to invoke this derogation by the data exporter is subject to numerous conditions that largely limit the scope of its application:

1) transfer shall not be repetitive;
2) it may take place only if transfer concerns a limited number of data subjects;[828]
3) the legitimate interest pursued by the controller must be "compelling";[829]
4) the compelling legitimate interest pursued by the controller shall not be "overridden by the interests or rights and freedoms of the data subject";[830]
5) the controller has provided "suitable safeguards" for the protection of the data concerned after having assessed the circumstances in which the transfer will be put in place;[831]
6) the controller should inform the supervisory authority and the data subject about the transfer.[832]

[828] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 15. No absolute threshold has been established thus making this condition highly dependent on the specific circumstances of the case.

[829] "For example, this might be the case if a data controller is compelled to transfer the personal data in order to protect its organization or systems from serious immediate harm or from a severe penalty which would seriously affect its business". Ibid., 15.

[830] Ibid., 16. The risk of a negative impact of data transfer on any interests/rights/freedoms of the data subject has to be assessed by the data exporter. As stated under Recital 75 GDPR, "[t]he risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage ...". As specified under Recital 113 GDPR, in assessing these risks – and in establishing what safeguards may be suitable to minimize those risks – the data exporter will need to consider "the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination".

[831] "As to the nature of such safeguards, it is not possible to set up general requirements applicable to all cases in this regard, but these will rather very much depend on the specific data transfer in question. Safeguards might include, depending on the case, for example measures aimed at ensuring deletion of the data as soon as possible after the transfer, or limiting the purposes for which the data may be processed following the transfer. Particular attention should be paid to whether it may be sufficient to transfer pseudonymized or encrypted data. Moreover, technical and organizational measures aimed at ensuring that the transferred data cannot be used for other purposes than those strictly foreseen by the data exporter should be examined". Ibid.

[832] Ibid., 16–17. This condition does not entail that the transfer shall be authorized by the supervisory authority. Rather, the duty to inform serves as an instrument that enables the supervisory authority to assess whether the transfer is appropriate and its impact on the rights and freedoms of the data subjects concerned. The data subject shall also be informed of such transfer as part of the obligation to inform the data subjects set out under Articles 13 ("Information to be provided where personal data are collected from the data subject") and 14 ("Information to be provided where personal data have not been obtained from the data subject").

Overall, the derogations analysed above seem to be unsuitable for framing international transfer on a large scale. The possibility to rely on consent, for example, is subject to a high threshold since several conditions will need to be met for consent to be a valid basis for transfer. For this reason, together with the fact that data subjects may withdraw their consent at any time, the EDPB itself has acknowledged that "consent might prove not to be a feasible long term solution for transfers to third countries".[833] In addition, when data are processed (and transferred) through the cloud, it may be particularly challenging for the data exporter to obtain consent for every single transfer from an EEA data centre to a non-EEA data centre and prove that consent was specific and informed.[834]

The derogations set out under Article 49(1)(b) (i.e., transfer based on the *necessity* to perform a contract between the data subject and the controller) and Article 49(1)(c) (i.e., transfer based on the *necessity* to conclude or perform a contract concluded in the interest of the data subject) are also unsuitable to cover transfers in the cloud: "[c]loud's efficiencies cannot 'necessitate' transfer to countries without adequate protection".[835] This has been confirmed by the ICO in stating that the derogation under Article 49(1)(b) "does not cover a transfer for [the data exporter] to use a cloud based IT system".[836] More broadly, the exceptional nature of the derogations under Article 49 GDPR seems incompatible with data transfers in the cloud where the flow of data can be easily qualified as "repetitive".[837] The possibility for the controller to invoke a compelling legitimate interest under Article 49(1) paragraph 2 is also likely to have a limited practical relevance considering its narrow scope of application.

[833] Ibid., 8. See also, McNabb and Klaebel Clemmensen, "GDPR Update: The Future of International Data Transfers."

[834] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 214.

[835] Ibid., 213.

[836] The ICO guidance on international transfers is available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers#admin.

[837] This opinion was expressed by the A29WP with reference to derogations under Article 26 of the Directive. "WP29 has adopted an opinion in which it considered that exemptions [under Article 26 DPD] shall apply only where transfers are neither recurrent, nor massive or structural. Based on such interpretations, it is almost impossible to rely on exemptions in the context of cloud computing". Article 29 Data Protection Working Party, *WP196*, 18.

5.7. Data Transfer Regime for Processors

Further uncertainties derive from the fact that, under the GDPR, data transfer requirements also apply to processors. Article 44 indeed prescribes that an international data transfer shall take place only if the conditions laid down under Chapter V "are complied with by the controller *and processor*".[838] Consistently, Article 46 GDPR prescribes that, in the absence of an adequacy decision, cross-border data transfer can take place if the controller *or the processor* has provided appropriate safeguards. The implementation of this provision may raise several questions when confronted with some practical scenarios:

1. A US data controller transfers data to an EEA data processor that further transfers data to a non-EEA data *processor* located in a non-adequate country:

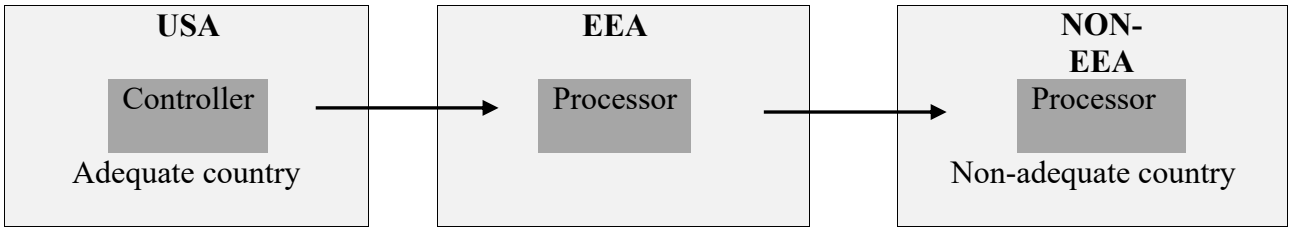

Table 7 – Data transfer regime for processors (scenario 1)

2. A US data controller transfers data to an EEA data processor that further transfers data to a non-EEA data *controller* located in a non-adequate country:

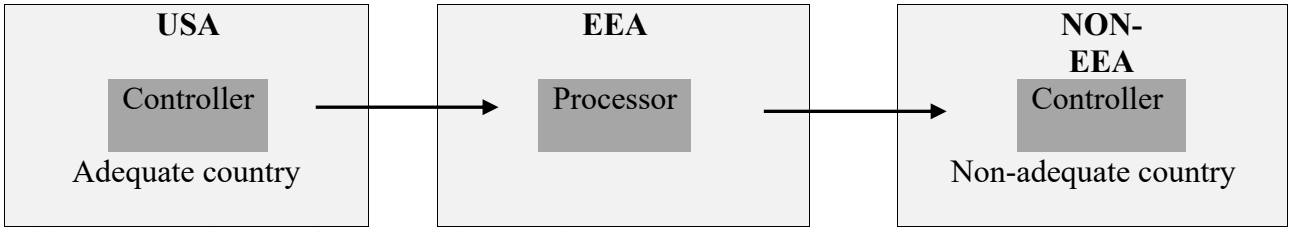

Table 8 – Data transfer regime for processors (scenario 2)

[838] Article 44 GDPR (italics mine).

3. a US data controller transfers data to an EEA data processor that then transfers the data *back* to the US data controller.

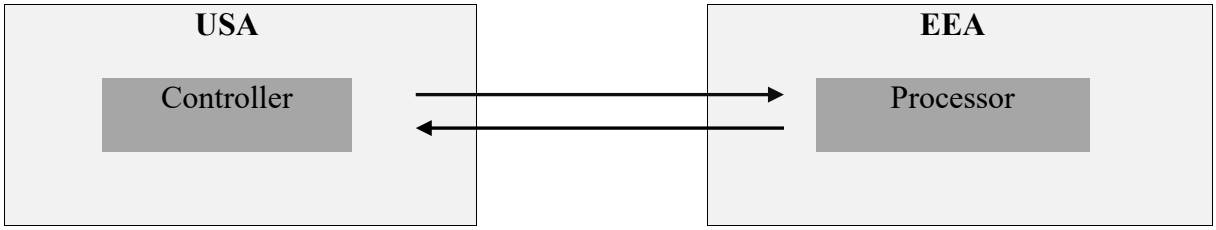

Table 9 – Data transfer regime for processors (scenario 3)

In all these scenarios, it is then necessary to distinguish (a) the case where the original US data controller is subject to the GDPR and (b) the case where it is not.[839]

In scenario 1, in the case where the US data controller is not subject to the EU jurisdiction (scenario 1.a), the EEA data processor will only be subject to *some* limited provisions that the GDPR directly imposes on processors (the so called "GDPR processor obligations" as seen in 3.3.4.). It should hence be concluded that in the event that the EEA data processor engages a non-EEA data processor in a non-adequate country, the latter should only be burdened with the obligations to which the EEA data processor is subject and not with the full scope of the Regulation. This, however, is not clearly reflected in the text of Article 46 GDPR that, by imposing on the processor the obligation to adduce "appropriate safeguards", seems to refer to the full scope of the Regulation. Moerel (2016) defines this as a "drafting mistake rather than a purposeful decision to deviate from this system" and suggests that the requirement under Article 46 GDPR should be interpreted as imposing on the data processor the obligation to provide appropriate safeguards "insofar as their own obligations are concerned only".[840]

On the other hand, in the event that the US data controller is subject to the GDPR (scenario 1.b), the whole data processing activities are governed by the GDPR and the data transfer provisions are already complied with by the US data controller in the moment the US data controller instructs

[839] Lokke Moerel, "GDPR Conundrums: Data Transfer," June 9, 2016, accessed August 7, 2018, https://iapp.org/news/a/gdpr-conundrums-data-transfer/.
[840] Ibid.

the EEA data processor to engage a non-EEA sub-processor. However, in this case, the GDPR does not clarify whether compliance with Article 46 GDPR on the part of the US data controller releases the EEA data processor from having to comply with data transfer provisions.[841] This seems to be the preferred interpretation especially considering that, pursuant to Article 46, "the controller *or* the processor" will need to provide appropriate safeguards,[842] thus implying that the requirement may be satisfied by either of the two parties involved.

Moving to scenario 2, the transfer would essentially take place from the US data controller to the non-EEA data controller passing through the EEA processor. In this framework, in the event that the US data controller is not subject to the GDPR (scenario 2.a), as in scenario 1.a, the choice made by the EU legislators is that the GDPR provisions does not apply to that processing while only some limited obligations will be imposed on the EEA data processor. Moerel (2016) hence suggested that, in this scenario, provisions on data transfer should not apply at all: "[r]equiring that if the EU processor transfers the data to the third-party controller the processor should impose requirements (either its own, or the full scope of the GDPR) on the controller is contrary to the intentions of the EU legislators".[843] On the other hand, in the event that the US data controller is subject to the GDPR (scenario 2.b), the same considerations made in scenario 1.b should apply, meaning that the data transfer provisions should not be complied with by the EEA processor since they should be implemented by the US data controller: "[i]mposing the data transfer rules on the data EU processor therefore has no added value".[844]

Lastly, in scenario 3, in the event that the US data controller is not subject to the GDPR (scenario 3.a.), as noted by Moerel (2016), data transfer provisions should not apply at all: "[o]therwise the result would be that a processor should impose requirements (either its own, or the full scope of the GDPR) upon the original controller, while the original processing was not governed

[841] Ibid.
[842] Article 46(1) GDPR (italics mine).
[843] Moerel, "GDPR Conundrums: Data Transfer."
[844] Ibid.

by the GDPR".[845] On the other hand, if the original US data controller is subject to the GDPR (scenario 3.b), the US controller is already subject to the full scope of the EU data protection legislation so that the implementation of data transfer mechanisms seem redundant. Again, data transfer provisions should not apply.[846]

This latter scenario (i.e., transfer of data from a non-EEA data controller to an EEA data processor that then transfers the data *back* to the original non-EEA data controller) has raised many uncertainties especially after that the EDPB has clarified that EEA data processors are required to comply the provisions on international data transfers even if the data controller on whose behalf they carry out the processing activities fall outside the scope of the GDPR (3.3.4.).[847] As noted by the Business Software Alliance in its response to the public consultation on the draft Guidelines 3/2018, "what grounds under [Chapter V] would actually be available in practice to enable transfers to non-EU data controllers" remains unclear. Indeed, current SCCs only cover controller-controller and controller-processor transfers and are hence unhelpful for framing transfers from EEA processors to non-EEA controllers.[848] This entails that if an adequacy decision does not cover the country where the non-EEA data controller is established and it is not possible to rely on a derogation, there is no other easy way to lawfully transfer the data.[849] On this point, the American Chamber of Commerce to the European Union stated that the silence by the EDPB – and the deriving legal uncertainties – on how data should be transferred from EEA processors to non-EEA controllers "is detrimental for both

[845] Ibid.
[846] Ibid.
[847] The list of the GDPR processor obligations, indeed, includes the provisions on international data transfer. European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 13.
[848] Business Software Alliance, *The Software Alliance's Response to the EDPB Public Consultation on the Proposed Guidelines on the Territorial Scope of the GDPR*, 2.
[849] City of London Law Society Data Law Committee, *Submission to the European Data Protection Board on Guidelines 3/2018*, 2019, 3, accessed May 2, 2019, http://www.citysolicitors.org.uk/attachments/category/186/CLLS%20Consultation%20Response%20on%20EDPB%20Territorial%20Scope%20Guidelines.pdf.

EU service providers and their non-EU customers" ,[850] thus making the need to design appropriate SCCs for processor-controller transfers a matter of urgency.[851]

The impossibility for EEA data processors to transfer data back to non-EEA controllers due to the unavailability of suitable legal bases for transfer may also lead to some paradoxical situations. In particular, this impossibility may put the EEA processor in the position of having to break the DP Agreement stipulated with the non-EEA controller. Indeed, under Article 28(3)(g) GDPR, the data processor shall delete or return "all the personal data to the controller after the end of the provision of services relating to processing".[852] In the absence of an adequacy decision for the country where the non-EEA controller is established and of any other suitable data transfer mechanism, the EEA data processor would hence be unable to return the data, which would inevitably put it in breach of its obligations under the DP Agreement.[853]

Looking more closely into scenario 3 (where data are first transferred from a non-EEA data controller to an EEA processor and then back to the original non-EEA data controller), it could be argued that such transfer does not even constitute an international data transfer within the scope of Chapter V GDPR but a *return* of the data to the original non-EEA data controller on whose behalf the EEA processor is processing the data. Indeed, theoretically, data are not transferred from the EU to third countries since the data concerned originated from the third country.[854] This opinion was put forward, among others, by Insurance Europe which noted that "should a non-EU controller engage an EU processor, the controller is the exporter and the processor is the importer. In that context, data transfer provisions should not apply because the data is imported into the EU and not exported outside

[850] American Chamber of Commerce to the European Union, *Our Position - Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, 3–4.

[851] Ibid., 4.

[852] Article 28(3)(g) GDPR.

[853] Insurance Europe, *Comments on the EDPB Guidelines on the GDPR Territorial Scope*, 2019, accessed May 3, 2019, https://www.insuranceeurope.eu/sites/default/files/attachments/Comments%20on%20the%20EDPB%20guidelines%20on%20the%20GDPR%20territorial%20scope.pdf.

[854] American Chamber of Commerce to the European Union, *Our Position - Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, 4.

the EU".[855] Along the same lines, Digital Europe maintained that data transfer mechanisms should not be needed when data are transferred from a non-EEA data controller to an EEA data processor and then back to the original non-EEA data controller since "such transfer merely restores the former state (the non-EEA data is with the non-EEA controller)".[856] Moreover, as highlighted by CILP, when the non-EEA data controller is not subject to the GDPR, applying data transfer provisions when data are transferred from the EEA processor to the original controller would have no added value to the protection of data subjects which have *never* benefitted from the protection of the GDPR by the non-EEA data controller.[857]

Needless to say, clarification is much needed.[858] Hopefully, such clarifications will take into account the need to connect jurisdiction to reasonableness (3.6.) and hence the need to avoid the applicability of EU data protection law to situations where there is a very limited connection with the

[855] Insurance Europe, *Comments on the EDPB Guidelines on the GDPR Territorial Scope*, 2.

[856] Digital Europe, *Response to Public Consultation on EDPB Draft Guidelines on Territorial Scope* (Brussels, 2019), 2, accessed May 2, 2019, https://www.digitaleurope.org/wp/wp-content/uploads/2019/01/DIGITALEUROPE-response-to-EDPB-territorial-scope-guidelines-FINAL.pdf. See also, Bitkom, *Views on EDPB Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, 9. Bird and Bird law firm also suggested that since controllers are "the ones who initiate the transfer, since they decide the purposes and means ... it may be that this is not a transfer from the EU but rather just a transfer *to* the EU – which is not restricted". Ariane Mole et al., "Where Does the GDPR Apply? European Data Protection Board Finally Weighs In," *Bird & Bird*, last modified November 2018, accessed May 3, 2019, http://www.twobirds.com/en/news/articles/2018/global/where-does-the-gdpr-apply-european-data-protection-board-finally-weighs-in.

[857] "Under Article 46(1) of the GDPR, international transfers can only happen 'on condition that enforceable data subject rights and effective legal remedies for data subjects are available', but these rights and remedies were never afforded to the non- EU data subjects in the first place. Applying Chapter V to these situations would not add any value to the protection of individual rights while putting unreasonable administrative burdens on EU processors". Centre for Information Policy Leadership, *Comments on the European Data Protection Board's "Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)" Adopted on 16 November 2018*, 10.

[858] In its response to the EDPB consultation on draft Guidelines 3/2018, the Personal Investment Management & Financial Advice Association ("PIMFA") regretted that the EDPB did not provide any detailed guidance on how EEA data processors can comply with their GDPR obligations when dealing with a non-EEA data controller that is not subject to the GDPR and, in particular, on how EEA data processors should implement data transfer provisions. Personal Investment Management & Financial Advice Association, *Response to the EDPB Consultation on Guidelines 3/2018 on the Territorial Scope of the GDPR*, 2019, 2, accessed May 2, 2019, https://www.pimfa.co.uk/wp-content/uploads/2019/01/PIMFA-response-to-EDPB-cp-on-guidelines-on-territorial-scope.pdf. See also the comment by Eduardo Ustaran (partner in the global Privacy and Cybersecurity practice of Hogan Lovells) on the EDPB draft guidelines 3/2018 on the territorial scope of the GDPR, where he noted that "...in relation to a situation where a non-EU controller engages an EU processor, the EDPB correctly points out that the processor will still be required to comply with the processor obligations imposed by the GDPR. The guidance that is missing is to what extent that processor needs to address – and how – the obligations in relation to international data transfers when the data is made available to the controller outside the EU". Eduardo Ustaran, "EDPB's Common Sense Approach to the GDPR's Territorial Scope," *Iapp*, November 26, 2018, accessed February 7, 2019, https://iapp.org/news/a/edpbs-common-sense-approach-to-the-gdprs-territorial-scope/.

EU. Some "safety valves"[859] should hence be introduced so as to avoid the *indirect* application of EU data protection rules – indirect application that derives from the implementation of data transfer mechanisms – in situations where the *direct* applicability of the EU data protection regime has been excluded by the EU legislators. This entails that in situations such as the one described in scenario 3, if the non-EU data controller is not caught under Article 3 GDPR (and hence does not fall under the *direct* applicability of the GDPR), data transfer rules should not apply to the transfer of data from the EU data processor to the non-EU data controller since the implementation of such rules would make the data protection principles *indirectly* applicable even if the processing as a whole is not governed by the Regulation.

5.8. Data Localization as a Last Resort?

Creating a regional cloud within the EU may be a relatively easy solution to avoid compliance with data transfer obligations, considering the administrative burdens and structural limitations that still hamper the resort to data transfer mechanisms, and the legal uncertainties that affect both old and new legal bases for transfer. Some cloud providers indeed offer their customers the possibility to select the region where their personal data will be stored. Among others:

Google	"Customer may select where certain Customer Data will be stored (the "Data Location Selection"), and Google will store it there in accordance with the Service Specific Terms. If a Data Location Selection is not covered by the Service Specific Terms (or a Data Location Selection is not made by Customer in respect of any Customer Data), Google may, subject to Section 10.2 (Transfers of Data Out of the EEA), store and process the relevant Customer Data anywhere Google or its Subprocessors maintains facilities".[860]
Amazon Web Services	"Customer may specify the location(s) where Customer Data will be processed within the AWS Network, including the EU (Dublin) Region, the EU (Frankfurt) Region, the EU (London) Region and the EU (Paris) Region (each a "Region"). Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body".[861]

[859] Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law," 241–242.

[860] Section 10.1, Google, Data Processing and Security Terms (Customers), accessed February 7, 2019, https://cloud.google.com/terms/data-processing-terms.

[861] Section 12.1, Amazon Web Services, GDPR Data Processing Addendum, accessed February 7, 2019, https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.

Rackspace	"In respect of data which the Customer receives, stores, or transmits on or using the Customer Configuration ... Customer may select the territory in which it stores and Processes Customer Personal Data ...".[862]
Oracle	"Personal Data held in Your Cloud Services environment will be hosted in the data center region specified in the Cloud Services Agreement or otherwise selected by You. Oracle will not migrate Your Cloud Services environment to a different data center region without Your prior written authorization".[863]
OVH UK	"In cases where the Services allow the Client to store content and notably Personal Data, the location(s) or, geographical area, of the available Datacenter(s) is specified on OVH Website. Should several locations or geographic areas be available, the Client shall select the one(s) of its choosing when submitting its Order. Subject to the applicable Special Terms of Service, OVH will not modify, without the Client's consent, the location or geographical area chosen when submitting its Order".[864]

Table 10 – Data location selection in cloud providers' DP Agreements

Interestingly, one of the OVH UK's main commitments to its customers in terms of data location is that when the customer selects the EU as a storage region, OVH will *never* process data in the US:

> When you select a storage region located in the EU, OVH guarantees that it will not process your data outside of the European Union, and any countries recognised by the European Commission as having a sufficient level of personal data protection regulations in place (with regard to the private lives, fundamental rights and freedoms of persons, and also with regard to exercising corresponding rights [adequacy decision]). We also guarantee that we will never process your data in the US.[865]

Certainly, the possibility to confine data within the EU region may be perceived by many GDPR-concerned customers as an attractive solution to avoid the risk of infringing data export restrictions.[866]

5.9. Restrictions to International Data Transfers and its Underlying Objectives

The analysis conducted above has shed light on the main legal uncertainties and structural problems that still affect the resort to the data transfer mechanisms under the GDPR. One could argue that these difficulties may be justified if those provisions succeed in achieving the objectives for which they have been designed. In Chapter 4, two main objectives underpinning data export restrictions have been identified: 1) preventing the circumvention of the EU data protection standards;

[862] Section 2.4 paragraph 2, Rackspace, Data Processing Addendum, accessed February 7, 2019, https://www.rackspace.com/sites/default/files/legal/rackspace-50186-v1-master_gsa_gdpr_dpa_jlf_220318_1.pdf.

[863] Section 7.1, Oracle, Data Processing Agreement for Oracle Cloud Services – v. July 27, 2018, accessed February 7, 2019, https://www.oracle.com/assets/data-processing-agreement-072718-5029569.pdf.

[864] Section 6 paragraph 1, OVH UK, Data Processing Agreement, accessed February 7, 2019, https://www.ovh.co.uk/support/termsofservice/Data%20Processing%20Agreement_UK.pdf.

[865] "GDPR - Our Expert Answers Your Questions – What Are OVH's Commitments in Terms of Data Location?," *OVH*, accessed February 7, 2019, https://www.ovh.co.uk/personal-data-protection/faq.xml.

[866] Hon and Millard, "How Do Restrictions on International Data Transfers Work in Clouds?," 274–275.

2) and preventing (indiscriminate) access on the part of foreign public authorities. It is now important to analyse to what extent data export restrictions meet these objectives.

5.9.1. Anti-circumvention Objective

As seen in Chapter 4, provisions on data transfer aim to ensure that "when the personal data of Europeans are transferred abroad, the protection travels with the data".[867] To achieve this aim, for example, contractual solutions as a basis for international data transfers "must provide additional safeguards for the data subject made necessary by the fact that the *recipient* in the third country is *not subject* to an enforceable set of *data protection rules* providing an adequate level of protection". The contract hence allows the data controller to provide for adequate safeguards "when transferring data *outside of the Community* (and thus *outside the protection* provided by the *directive*, and indeed by the general framework of Community law) to a third country where the general level of protection is not adequate".[868]

On this ground, it could be argued that the implementation of data transfer mechanisms is redundant when data are transferred to a non-EEA recipient that is *directly* subject to the EU data protection legislation by virtue of the extraterritorial reach of the GDPR. After all, if the processing of transferred personal data can continue to be carried out compliantly with the EU data protection principles, the anticircumvention aim could be achieved without restricting data flow. Indeed, as a normative matter, the risk that data will be processed "unlawfully" only arises when the natural or legal person receiving and subsequently processing those data is *not* legally bound to comply with the data protection standards prescribed under the EU data protection legislation. And considering the broad (extra)territorial reach of the GDPR (and of the DPD before it), we can expect that similar situations will be limited to some marginal cases (e.g., transfer from an EEA controller to a non-EEA controller that has *no* establishment in the EEA, that is *not* offering goods or services to data subjects

[867] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 4.
[868] Article 29 Data Protection Working Party, *WP12*, 16 (italics mine).

in the EU and that does *not* deploy any online or offline tools, not even cookies, to monitor individuals in the EU).

I will call this approach "jurisdictional approach" since, in determining whether transfer should be restricted or not, it focuses on the jurisdiction to which the recipient is subject rather than on data location *per se*. Interestingly, this approach seems to be followed by Convention 108+ which has replaced *territory* with *jurisdiction* in the Article that covers transborder flows of personal data. Indeed, as seen in Chapter 4 (4.3.), Article 14(2) of Convention 108+ does no longer refer to international data transfer as the movement of data from the *territory* of one country to the *territory* of another country. Rather, Article 14(2) refers to the transfer of personal data to a recipient that "is *subject* to the *jurisdiction* of a State or international organisation which is *not Party* to this Convention".[869] This does not entail that territory is losing its relevance but this change may suggest that, in assessing the risks to which data are exposed in the event of an international data transfer, the territory in which the recipient is located is *one* factor to be taken into consideration together with other factors, *in primis*, the jurisdiction to which the recipient is subject.

This seeming inconsistency between the rules that define the territorial scope of the EU data protection legislation on the one hand, and data transfer rules on the other was pointed out by Kuner back in 2007: "[i]t should not be necessary to comply with the Articles 25 and 26 when EU law applies anyway by virtue of Article 4 of the ... Directive".[870] Indeed, "if EU data protection law, with its panoply of protections, applies to a particular act of data processing on the internet because of the use of automated equipment, then what is the need for subjecting such processing to data transfer restrictions as well ...?". Along the same lines, "...a member of safe harbor in the US that also used cookies on its website could find that its US processing of European user data was subject to both the safe harbor principles and the applicable Member State law as determined by Article 4 [of the Directive]".[871] Kuner hence criticized the existence of two overlapping but uncoordinated sets of

[869] Article 14(2) Convention 108+ (italics mine).
[870] Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 167.
[871] Ibid.

requirements both aimed at avoiding the circumvention of the EU data protection standards. In order to avoid the simultaneous application of "rules regulating transborder data flows (ie Articles 25 and 26) in situations where EU law applies anyway (ie under Article 4) or vice versa", Kuner suggested that "the dual regime under Articles 4, 25, and 26" is replaced by "a single regime to protect personal data processed outside the EU".[872]

The need to overcome (or at least clarify) this overlap between the jurisdictional regime of the GDPR set out under Article 3 on the one hand, and the data transfer regime on the other has been expressed, among others, by CIPL on 18 January 2019, in its comments on the EDPB's Draft Guidelines 3/2018 on the territorial scope of the GDPR:

> In essence, an accumulation of the obligations under Article 3(2) of the GDPR and Chapter V of the GDPR would not make sense. An organisation acting within the scope of Article 3(2) is required to put in place all the measures and safeguards of the GDPR. There is no added value in requiring this organisation to additionally comply with the obligations of Articles 46, 47 and 49 of the GDPR, because the organisation is already bound by all obligations stemming from these latter provisions.[873]

CIPL argued that not only is an accumulation of several demanding layers of compliance unnecessary but it may also "ultimately run counter to operational compliance and accountability".[874] CIPL even suggested that if a non-EEA recipient proactively commits to abide by the GDPR standards – supposedly, even in the event that the non-EEA recipient is not legally bound to do – these commitments should be leveraged in order to be free from the obligation to comply with the data transfer provisions.[875]

---

[872] Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law," 244. In this article, Kuner noted that "[q]uestions can ... be raised about the consistency of Articles 25 and 26 with Article 4 of the Directive (the article that regulates applicable law). Articles 25 and 26 are supposed to result in protection being provided to personal data transferred to third countries, where by definition EU law does not apply, and the primary policy behind them is to avoid the circumvention of EU data protection standards. However, there are many cases involving data transfers where EU law applies directly under Article 4. For example, Article 29 Working Party has found that EU law applies under Article 4(1)(c) of the Directive when an individual in the EU enters data in an Internet search engine or uploads data onto an online social network operated from a server in another region, in which situation personal data are obviously flowing from the EU to third countries. In practice, there are many companies that have applied adequate safeguards (such as conclusion of the EU standard contractual clauses) or have joined the EU–US Safe Harbor, even though EU data protection law applies to them directly under Article 4" (p. 244). On this point, see also Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, 42–43.

[873] Centre for Information Policy Leadership, *Comments on the European Data Protection Board's "Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)" Adopted on 16 November 2018*, 19.

[874] Ibid.

[875] Ibid., 21.

A similar view was expressed by the Personal Investment Management & Financial Advice Association (PIMFA) in its response to the EDPB's draft Guidelines 3/2018. PIMFA suggested that since some controllers and processors established outside the EEA will be caught under the territorial scope of the GDPR, "it is arguable that any transfer of data to such controllers and processors would *not be restricted data* and hence the additional measures required by Chapter V of the GDPR would *not apply*".[876] This conclusion would clearly facilitate international data transfer especially considering that, as noted by PIMFA, the implementation of data transfer measures is often rather challenging especially when data exporters cannot rely on the derogations set out under Article 49 and when there is no separate legal entity with which the data exporters can enter into SCCs[877] (5.5.1.2.).

The interplay between Article 3 and Chapter V GDPR was also addressed by the Internet Corporation for Assigned Names and Numbers (ICANN) in its correspondence with the Belgian DPA. In particular, in its letter of 6 December 2018 directed to both the Belgian DPA and the Irish Data Protection Commission, ICANN noted the following:

> Pursuant to Art. 44 GDPR transfer safeguards, such as Standard Contractual Clauses, are required only with regard to transfers to data recipients located in third countries (i.e. countries outside of the EEA), or in case of international organizations as the data recipients, where such importers are not subject to direct application of the GDPR. If data recipients in third countries are already in the direct scope of applicability of the GDPR, such transfer safeguards will not be required.[878]

On this ground, ICANN argued that since it is directly subject to the GDPR by virtue of Article 3, no data transfer mechanisms would need to be implemented in order to enable the transfer of data from the EEA, precisely from ICANN's Brussels office to ICANN's offices outside the EEA. After all,

---

[876] Personal Investment Management & Financial Advice Association, *Response to the EDPB Consultation on Guidelines 3/2018 on the Territorial Scope of the GDPR*, 2 (italics mine).

[877] Ibid., 2. The City of London Law Society (CLLS) is also in favour of ruling out the applicability of data transfer provisions when transferring data to data importer that are directly subject to the GDPR. On this point, see City of London Law Society Data Law Committee, *Submission to the European Data Protection Board on Guidelines 3/2018*, 7.

[878] *Letter from Marby Göran, ICANN's President and Chief Executive Officer, to Willem Debeuckelaere, President of the Belgian Data Protection Authority and to Helen Dixon, Data Protection Commissioner for Ireland*, 2018, 2, accessed March 11, 2019, https://www.icann.org/en/system/files/correspondence/marby-to-debeuckelaere-dixon-06dec18-en.pdf.

"[i]f the GDPR directly applies, the level of data protection required under the GDPR is ensured".[879] This approach was, however, ruled out by the Belgian DPA which responded to ICANN's letter by stating that "article 44 and following of the GDPR do *not* stipulate that appropriate safeguards shall *no longer* be necessary in case where the GDPR is directly applicable to the recipient of the data". Rather, Chapter V applies to *any* international data transfers while the only derogations to this general principle can be found under Article 49 ("derogations for specific situations" analysed in 5.6.).[880]

The ICO seems to have adopted a different view from the one expressed, although informally, by the Belgian DPA. Indeed, in its guidelines on international transfers, it clarified that an international data transfer is restricted under the GDPR when the data exporter is "sending personal data, or making it accessible, to a receiver to which the GDPR does not apply. Usually because they are located in a country outside the EEA".[881] The ICO seems hence to place more attention on the *jurisdiction* to which the data recipient is subject more than over *data location per se*.[882] Interestingly, a similar view was also expressed at the 12th edition of the Computers, Privacy and Data Protection Conference that was held in Brussels from 30 January to 1 February 2019, by Jos Dumortier, an Honorary Professor of ICT Law at the University of Leuven and partner at Timelex, who suggested that Article 46 should not be considered as providing an exhaustive list of "appropriate safeguards".

---

[879] Ibid.

[880] *Letter from Willem Debeuckelaere, President of the Belgian Data Protection Authority, to Göran Marby, ICANN's President and Chief Executive Officer*, 2019, 2 (italics mine), accessed March 11, 2019, https://www.icann.org/en/system/files/correspondence/debeuckelaere-to-marby-15jan19-en.pdf. In its response letter, ICANN took "note of the provisional and informal view taken by the Belgian supervisory authority (based on information available to date) that the GDPR does not stipulate that appropriate safeguards are not necessary in the case where the GDPR is directly applicable to the recipient of the data. ICANN will further consider this position in the light of the current and future positions or views of other European supervisory authorities and the upcoming final version of the European Data Protection Board guidelines on the scope of the GDPR". See, *Letter from Göran Marby, ICANN's President and Chief Executive Office, to William Debeuckelaere, President of the Belgium Data Protection Authority*, 2019, 3–4, accessed March 11, 2019, https://www.icann.org/en/system/files/correspondence/marby-to-debeuckelaere-25jan19-en.pdf.

[881] The ICO guidance on international transfers is available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers#admin.

[882] "So, if a non-EEA data importer receives personal data from the EEA, the processing of which will, for the data importer, be subject to the extra-territorial reach of the GDPR, a form of 'protective bubble' applies to that processing which means that it is not a restricted transfer, and the mechanisms in Chapter V which are necessary to ensure an adequate level of protection (e.g. the use of standard contractual clauses) do not need to be considered". James Clark and Natalie Webb, "ICO Clarifies Position in Respect of International Transfers under the GDPR," *Privacy Matters - DLA Piper*, September 12, 2018, accessed February 8, 2019, https://blogs.dlapiper.com/privacymatters/uk-ico-clarifies-position-in-respect-of-international-transfers-under-the-gdpr/.

Rather, "appropriate safeguards", as a legal basis for transfer, may also be represented by the fact that the non-EEA data recipient is directly subject to the GDPR.[883]

The EDPS seems to have pointed to the same "mismatch" between the direct applicability of the EU data protection legislation and data transfer provisions when, two days before that the GDPR became applicable, he noted that the "Privacy Shield is still there but is less relevant … because the entire set of standards, including the transfer, should be subject to higher standards". "On Friday [25 May 2018], what you do in Europe remotely is subject to GDPR in its entirety".[884] The EDPS reiterated a similar concept at the presentation to the media of the EDPS's 2018 Annual Report on 26 February 2019, when he said that the Privacy Shield should be considered as an "interim instrument looking to the past and not the future". The GDPR applies to everybody working remotely in the EU by profiling people or offering goods and services. This entails that a company that is subject to the full scope of the GDPR "should respect the GDPR in its entirety and not only when the data are transferred".[885]

In the light of the above, it can be concluded that the jurisdictional approach to data transfer is starting to gain ground at various levels. This is certainly a sensible approach since its implementation and development would allow to get rid of some of the purely formal requirements that, under the GDPR, unduly restrict data transfers even when the GDPR directly and fully apply to the non-EEA data recipient. However, as it will be argued in greater detail in the next chapter, the adoption of a similar approach – or at least the adoption of such approach without some fine-tuning

[883] Dumortier Jos, "How the Adequacy Mechanism Works: Progress in the EU's Governance of Cross-Border Data Flows?" (Presented at the Computers, Privacy and Data Protection conference, Brussels, January 30, 2019). Mr Dumortier presented the case of a Japanese company with several subsidiaries all over the EEA. All the subsidiaries can be qualified as processors while the Japanese company is the controller. Data are transferred from the EEA subsidiaries to the Japanese headquarter. The Japanese company is fully bound by the provisions of the GDPR regardless of the presence of an adequacy decision by virtue of Article 3(1) GDPR since the processing activities conducted by the Japanese company are carried out in the context of the activities of the EEA establishments (i.e., the EEA subsidiaries) of the Japanese company. A legal basis for transfer should be identified since data are transferred from the EEA entities to the Japanese company. According to Mr Dumortier, in this case appropriate safeguards may be represented by the fact that the Japanese company is fully bound by the GDPR.

[884] Giovanni Buttarelli, quoted in Nikolaj Nielsen, "Privacy Shield Less Relevant given GDPR, Says Data Chief," *EUobserver*, May 24, 2018, accessed May 26, 2018, https://euobserver.com/justice/141886.

[885] Giovanni Buttarelli's presentation to the media of the EDPS's 2018 Annual Report on 26 February 2019 is available at: https://www.youtube.com/watch?v=R_2XT79AeAw.

– may come with some practical inconveniences (in particular, when data are transferred from EEA controllers to non-EEA controllers) as well as with some inefficiencies in protecting data (since direct applicability of the EU data protection legislation does not always guarantee effective implementation of such legislation). What is sure is that the need to untangle the interplay between the (extra)territorial scope of the GDPR and data transfer mechanisms has now become a pressing issue. Not by chance, as it emerges from the agenda of the 6th EDPB meeting (22-23 January 2019), the EDPB has established an expert subgroup on the "Interplay between Art. 3 GDPR and Chapter V of the GDPR".[886]

5.9.2. Preventing Access by Foreign Public Authorities

Besides avoiding the circumvention of the EU data protection standards, data transfer restrictions also aim to avoid that the non-EEA data recipient is subject to disclosure requests that go beyond what is necessary in a democratic society. This "fear" is based on the assumption that the transfer of data to third countries will *increase* the exposure of those data to disclosure requests from law enforcement authorities, or to direct seizure on the part of intelligence activities. However, recent developments show that data location is increasingly losing its relevance as a connecting factor in both the law enforcement and the intelligence fields, meaning that restricting data flow or suspending the transfer of data may play little or no role in protecting data from foreign public authorities.

With regards to the surveillance activities conducted by intelligence services, as seen above (2.4.), intelligence services may easily gain (indiscriminate) access to data, no matter where data are located by means of remote *direct* seizure of data (e.g., hacking and wiretapping)[887] or by means of data sharing arrangements between EU and non-EU intelligence services. Indeed, on the one hand,

[886] The agenda of the 6th EDPB meeting (January 22-23, 2019) is available at: https://edpb.europa.eu/sites/edpb/files/files/file1/20190122plen-_agenda_-public_version_en.pdf. See also the agenda of the 9th EDPB meeting (April 9, 2019) which lists the "Interplay between Art. 3 GDPR and Chapter V" among the current focuses of the EDPB, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/20190408plenpublicagenda_en.pdf.

[887] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 141.

surveillance activities are often conducted by intelligence agencies outside their country's borders[888] and it is hence doubtful that the place of data storage may affect the technical capabilities of intelligence services to gain access to those data.[889] On the other hand, considering the widespread information sharing programs conducted between intelligence services of different countries, once data have been accessed by the agency of one country, they may then be passed on to the agencies of other countries "so that the place of the computer where data are stored may be largely irrelevant to whether they can be accessed by the intelligence services".[890]

Data location is also losing its relevance in the law enforcement sphere as witnessed by the adoption in March 2018 by the US Congress of the Clarifying Lawful Overseas Use of Data (CLOUD) Act.[891] The aim of the Cloud Act is to enhance United States' and its foreign partners'

[888] As highlighted by the EDPB in its second annual joint review on the Privacy Shield, when assessing the adequacy of a third-country legal framework in protecting data, the analysis should not be limited to the legal grounds that allow public authorities to conduct surveillance within that country's borders "but should also include an analysis of the legal grounds in that third country's law which allow it to conduct surveillance outside its territory as far as EU data are concerned". European Data Protection Board, *EU-U.S. Privacy Shield - Second Annual Joint Review*, 17.

[889] Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," 915.

[890] Ibid.

[891] *Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 23 March 2018* (H.R. 4943, 2018). A wide debate has sparked from the adoption of the Cloud Act as to whether it protects or, rather, threatens privacy. Electronic Frontier Foundation, for example, strongly contested the adoption of the Cloud Act: "[b]ecause of this failure, U.S. and foreign police will have new mechanisms to seize data across the globe. Because of this failure, your private emails, your online chats, your Facebook, Google, Flickr photos, your Snapchat videos, your private lives online, your moments shared digitally between only those you trust, will be open to foreign law enforcement without a warrant and with few restrictions on using and sharing your information. Because of this failure, U.S. laws will be bypassed on U.S. soil". David Ruiz, "Responsibility Deflected, the CLOUD Act Passes," *Electronic Frontier Foundation*, last modified March 22, 2018, accessed May 6, 2019, https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes.
The American Civil Liberties Union and other organizations, in a coalition letter to the US Members of Congress, also strongly opposed the adoption of the Cloud Act, claiming, among others, that the legislation would "[a]llow foreign governments to wiretap on U.S. soil under standards that do not comply with U.S. law; Give the executive branch the power to enter into foreign agreements without Congressional approval; Possibly facilitate foreign government access to information that is used to commit human rights abuses, like torture; and Allow foreign governments to obtain information that could pertain to individuals in the U.S. without meeting constitutional standards". *Coalition Letter from American Civil Liberties Union et al. to US Members of Congress of 12 March 2018*, 2018, accessed May 6, 2019, https://www.aclu.org/sites/default/files/field_document/cloud_act_coalition_letter_3-8_clean.pdf.
On the other hand, some leading US tech companies shared their support for the adoption of this new piece of legislation in stating that the Cloud Act "reflects a growing consensus in favor of protecting Internet users around the world and provides a logical solution for governing cross-border access to data". *Letter from Apple, Facebook, Google, Microsoft and Oath to Senators of the US Congress Orrin Hatch, Christopher Coons, Lindsey Graham, and Sheldon Whitehouse of 6 February 2018*, 2018, accessed May 6, 2019, https://blogs.microsoft.com/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf.
See also the statement from Brad Smith, Microsoft President, on the inclusion of the CLOUD Act in the Omnibus funding bill: "Today is an important day for privacy rights around the world, for international relations and for building trust in the technology we all rely on every day ... The proposed CLOUD Act creates a modern legal framework for how law enforcement agencies can access data across borders ... while ensuring appropriate protections for privacy and human rights. And it gives tech companies like Microsoft the ability to stand up for the privacy rights of our customers around

capability to access electronic information held by US-based communications services providers (CSPs) regardless of the location of the information requested. The adoption of the Cloud Act was mainly driven by the weaknesses of current instruments, especially MLATs, in giving law enforcement authorities swift access to electronic data held in foreign jurisdictions (2.3.). Indeed, in a context where many CSPs operate at a global level with offices and facilities all over the world, and where data are stored, moved and even split in multiple countries,

> it can be impossible for investigating governments to submit multiple MLAT requests to multiple foreign governments to obtain electronic data scattered in multiple countries, especially when the governments (and sometimes even the CSPs themselves) do not know where the data is stored and when the data may well have been moved to another location by the time the requests are reviewed.[892]

Simply put, data location is no longer a suitable basis for grounding requests to disclose electronic data and, according to the US Department of Justice, "[f]ailing to address this situation would increase incentives for data localization across the world, which would harm both global commerce and public safety".[893]

More specifically, the Cloud Act introduces two major changes. Firstly, the Cloud Act *clarifies*[894] that CSPs subject to the US jurisdiction[895] can be compelled by US authorities to produce data in their possession regardless of where those data are stored. The Cloud Act has, in fact, amended

---

the world". Brad Smith, *Statement of 21 March 2018 on the Inclusion of the CLOUD Act in the Omnibus Funding Bill*, 2018, accessed May 6, 2019, https://perma.cc/QKN2-H5W5.
Support for the Cloud Act has also been expressed among established privacy scholars. Among others, Jennifer Daskal and Peter Swire claimed that "the bill would improve privacy and civil liberties protections compared to a world without such legislation". Jennifer Daskal and Peter Swire, "Why the CLOUD Act Is Good for Privacy and Human Rights," *Lawfare*, March 14, 2018, accessed May 6, 2019, https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

[892] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, 2019, 9, accessed May 6, 2019, https://www.justice.gov/dag/page/file/1153436/download.

[893] Ibid.

[894] Ibid., 8. The US Department of Justice stressed that the Cloud Act does not give US authorities *new* powers to acquire data but it *confirms* the scope of application of the SCA.

[895] As explained by the US Department of Justice, "the United States must have personal jurisdiction over a company in order to require the disclosure of information the company holds ... Personal jurisdiction is most readily established when a company is located in the United States. Whether a foreign company located outside the United States but providing services in the United States has sufficient contacts with the United States to be subject to U.S. jurisdiction is a fact-specific inquiry turning on the nature, quantity, and quality of the company's contacts with the United States. The more a company has purposefully directed its conduct into the United States, the more likely a court will find the company is subject to U.S. jurisdiction". Ibid.

the Stored Communications Act (SCA), the federal statute that empowers US investigators to compel CSPs subject to the US jurisdiction to disclose data in their control, by adding the following sentence:

> A provider of electronic communication service or remote computing service shall 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, regardless of whether such communication, record, or other information is located within or outside of the United States.[896]

This amendment was approved to resolve the questions raised by the so-called *Microsoft* case about the applicability of the SCA to data that companies subject to the US jurisdiction have stored abroad. Disagreements about the (territorial) scope of SCA arose after that, in the aforementioned *Microsoft* case, the US Court of Appeals for the Second Circuit held that the SCA did not give to the US government the authority to require Microsoft to disclose data that it had stored in servers located in Ireland, and hence outside the US borders.[897] This decision was then appealed to the US Supreme Court but, before a decision was made, the Cloud Act was enacted thus mooting the case.[898]

The Cloud Act has certainly provided an easy "fix" to the *Microsoft* case and to other similar cases that will surely continue to arise. It should however be noted that the "irrelevance" of data location upon which the Cloud Act is grounded is likely to clash with the location-centred provisions set out under Chapter V of the GDPR. In particular, Article 48 GDPR provides that any "judgment of a court or tribunal and any decision of an administrative authority of a third country" shall be recognized only on the basis of an international agreement and that such transfer shall occur "without prejudice to other grounds for transfer pursuant to" Chapter V of the GDPR.[899] Article 48 GDPR hence provides that disclosure requests by foreign public authorities do not legitimize *per se* the transfer of the requested data. In the absence of an international agreement and of another legal basis

---

[896] §2713 Cloud Act.

[897] *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016).

[898] For a more detailed analysis of the *Microsoft* case, see Jennifer Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0," *Stanford Law Review Online* 71, no. 9 (2018): 9–11, accessed May 6, 2019, https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/; Secil Bilgic, "Something Old, Something New, and Something Moot: The Privacy Crisis Under the Cloud Act," *Harvard Journal of Law & Technology* 32, no. 1 (2018): 331–333.

[899] Article 48 GDPR.

under the GDPR,[900] EU companies should hence generally refuse to comply with direct requests by foreign authorities.[901] This inconsistency between the approach adopted by the Cloud Act, which moves away from data location as a connecting factor, and the location-centred approach adopted by the GDPR may generate conflicts between the two legal orders.[902] Such conflicts may be overcome thanks to the negotiations that the European Union has started with the US government following the Commission's Recommendation for a Council Decision authorising the opening of negotiations with the US on cross-border access to electronic evidence that was issued on 5 February 2019 (see further below in this paragraph).

The second part of the Cloud Act addresses the reversed problem that is often faced by foreign countries when seeking access to data held by US-based CSPs. Precisely, the Cloud Act authorizes the United States to stipulate executive agreements with other countries as a means to remove the conflict-of-law problems that US-based providers face when they receive disclosure orders by other countries. This conflict of laws derives from the fact that CSPs are often subject to the laws of several countries: they might receive the order to disclose some data in their control by the authorities of country A and, at the same time, be subject to the law of country B that prohibits such disclosure either because the data concerned are located in country B, or because producing those data would require to take action in that country, or because the requested data pertains to country B's citizens. When facing similar conflicting orders, CSPs need to decide which law to follow and which one to break.[903]

Taking into account these situations, the executive agreements stipulated under the Cloud Act can be used to *lift* the conflicting requirements under each country's laws in order to allow CSPs to

[900] The transfer could be framed under Article 49 GDPR, but the high thresholds set in this Article are hard to be met.

[901] European Data Protection Supervisor and European Data Protection Board, *Initial Legal Assessment of the Impact of the US CLOUD Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-Border Access to Electronic Evidence* (Brussels, 2019), 3, accessed December 14, 2019, https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.

[902] Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0," 11–12.

[903] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, 2–3.

comply with the disclosure requests from other countries without the risk of facing potential liabilities under US law. As explained by the US Department of Justice, by eliminating these conflicts of law, the "CLOUD Act enables the United States to *help* its foreign law enforcement partners obtain electronic evidence from global CSPs based in the United States that [its] partners need for their investigations of serious crime".[904] At the same time, it should be recalled that these executive agreements are meant to supplement, and *not* replace, other existing legal instruments for acquiring data held in foreign jurisdictions, like MLATs.[905]

The need to facilitate and speed up law enforcement access to electronic evidence has also been perceived at the EU level where "almost two thirds of crimes where electronic evidence is held in another country cannot be properly investigated or prosecuted, mainly due to the time it takes to gather such evidence or due to fragmentation of the legal framework".[906] This is why, on 17 April 2018, the European Commission presented a package of legislative proposals on e-evidence after having conducted an impact assessment where it defined and analysed the problem(s) related to the

[904] Ibid., 4 (italics mine).

[905] Ibid., 5. However, the Cloud Act prescribes that the executive agreements shall require that "the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement" (§ 2523(b)(4)(A)) and that "the foreign government may not target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States" (§ 2523(b)(4)(B)). This entails that, since in such situations the sought-after data cannot be obtained by means of an executive agreement under the Cloud Act, the MLAT system will continue to apply. On this point, see Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0," 14.

[906] European Commission - Press release, "Security Union: Commission Facilitates Access to Electronic Evidence," last modified April 17, 2018, accessed May 9, 2019, http://europa.eu/rapid/press-release_IP-18-3343_en.htm.

cross-border access to data[907] and where it conducted both a qualitative (i.e., a social, economic and fundamental rights assessment) and a quantitative assessment of the available policy options.[908]

The overall aim of the proposals is to facilitate access to e-evidence by allowing the judicial authorities of one Member State to request access to evidence directly from a service provider in another Member State irrespective of where the sought-after data are saved. The new rules hence aim to create a fast-track for access requests by replacing cooperation with the public authorities of another Member State with *direct* cooperation with the service providers that are in control of the requested data. Moreover, the proposed rules may have the desirable result of increasing legal certainty for both law enforcement authorities and service providers since the cooperation on the part of service providers would be no longer provided on a voluntary basis but would be made mandatory.[909] The package of legislative proposals is composed of a proposal for (1) a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matter,[910] and of a proposal for (2) a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[911]

---

[907] The European Commission identified three main channels for obtaining access to data stored in foreign jurisdictions: "1. judicial cooperation between public authorities, 2. direct cooperation between a public authority and a service provider and 3. direct access to electronic evidence by a public authority". However, all these channels suffer from limitations: "judicial cooperation is often too slow for timely access to data and can entail a disproportionate expense of resources; direct cooperation can be unreliable, is only possible with a limited number of service providers which all apply different policies, is not transparent and lacks accountability; legal fragmentation abounds, increasing costs on all sides; and the size of the problem is steadily increasing, creating further delays". European Commission, *Commission Staff Working Document. Impact Assessment, Accompanying the Document 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 Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, SWD(2018) 118 final. (Brussels, 2018), paragraph 2.1.1., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN.

[908] The public consultation on e-evidence was open from 4 August 2017 to 27 October 2017. The report is available at the following link: https://ec.europa.eu/info/sites/info/files/report_of_open_public_consultation_on_e_evidence_april2018.pdf.

[909] European Commission, *Frequently Asked Questions: New EU Rules to Obtain Electronic Evidence* (Brussels, 2018), accessed May 7, 2019, http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm.

[910] 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), 2018).

[911] European Commission, *Proposal for a Directive of the European Parliament and of the Council Laying down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings* (COM/2018/226 final - 2018/0107 (COD), 2018).

The proposed Regulation will create a European Production Order and a European Preservation Order. The European Production Order will allow the judicial authorities in a Member State to request access to data to the service provider or to its representative in another Member State. On the other hand, the European Preservation Order will allow a judicial authority in a Member State to prevent the service provider or its legal representative in another Member State from deleting or altering some specific data in the view of a future European Production Order or of a request to produce the data via MLATs. The most relevant novelty of the proposed Regulation (at least for the sake of this Chapter) is that it "moves away from data location as a determining connecting factor". This "move" is motivated by the fact that "data storage normally does not result in any control by the state on whose territory data is stored". Rather, "such storage is determined in most cases by the provider alone, on the basis of business considerations".[912]

Data location as a connecting factor is replaced by the presence of a "sufficient conjunction between the provider and the territory where it is offering its services". Indeed, Article 3 of the proposal clarifies that the Regulation "applies to all service providers that *offer* services in the Union", meaning that they enable "legal or natural persons in one or more Member States to use its services". At the same time, "the mere accessibility of the service ... should not be a sufficient condition for the application of this Regulation. Therefore, a substantial connection to those Member States is required to ascertain a sufficient conjunction between the provider and the territory where it is offering its services".[913]

The Directive will complement the Regulation by imposing on all service providers that offer services in the EU the obligation to appoint a legal representative in the EU which will be responsible

[912] Article 1, 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*.

[913] Article 3 (italics mine), Ibid. For a critical assessment of this "deterritorialisation of data" see the 2018 study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee: Martin Böse, *An Assessment of the Commission's Proposals on Electronic Evidence*, 2018, 33–34, accessed May 7, 2019, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf. See also European Data Protection Board, *Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Art. 70.1.b)*, 2018, 8–9, accessed December 15, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf.

for receiving and complying with the European Production and Preservation orders. The main aim of the Directive is hence "to identify the addressee of the orders of Member States' authorities to obtain evidence in criminal matters held by service providers". This would offer "a common, EU-wide solution for addressing legal orders to service providers by way of a legal representative".[914] As for the location of the legal representative, Article 3 of the Proposal provides that service providers should appoint their legal representative in the Member State where they are established or where they offer services.[915]

Moreover, on 5 February 2019, the European Commission issued a recommendation for a Council decision authorizing the opening of negotiations with the US (where most of the service providers are headquartered) in order to complement the *EU* package of legislative proposals on e-evidence with *international* rules on cross-border access to data.[916] The said recommendation was adopted following the European Council Conclusions of 18 October 2018, where the European Council urged the European Commission to "submit negotiating mandates for the international negotiations on e-evidence".[917]

---

[914] European Commission, *Proposal for a Directive of the European Parliament and of the Council Laying down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, 3.

[915] Article 3(1), European Commission, *Proposal for a Directive of the European Parliament and of the Council Laying down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*.

[916] European Commission, *Explanatory Memorandum - Recommendation for a Council Decision Authorising 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. (Brussels, 2019), accessed May 7, 2019, https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf. See also, European Commission - Press release, "Questions and Answers: Mandate for the EU-U.S. Cooperation on Electronic Evidence," last modified February 5, 2019, accessed May 9, 2019, http://europa.eu/rapid/press-release_MEMO-19-863_en.htm. For a critical analysis of the Commission's negotiation mandate see, European Data Protection Supervisor, *Opinion 2/2019 on the Negotiating Mandate of an EU-US Agreement on Cross-Border Access to Electronic Evidence*, 2019, accessed December 15, 2019, https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf.

[917] European Council, *European Council Meeting (18 October 2018) - Conclusions*, EUCO 13/18. (Brussels, 2018), 3, accessed May 7, 2019, https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf. See also the outcome of the Council of the European Union meeting (Justice and Home Affairs) held on 4 and 5 June 2018: "During the debate, ministers exchanged views on: ... the current international developments on e-evidence and, in particular, the impact of the US CLOUD Act adopted in March 2018. On the latter, the Council confirmed the common EU approach towards the US regarding the conclusion of an executive agreement under the US CLOD Act. The Council asked the Commission to continue contacts with the US authorities and to urgently submit a negotiation mandate, if possible before the summer recess". Council of the European Union, *Outcome of the Council Meeting*, 3622nd Council meeting, Justice and Home Affairs, 9680/18. (Luxembourg, 2018), 19, accessed May 7, 2019, https://www.consilium.europa.eu/media/35542/st09680-en18.pdf.

According to the European Commission, these negotiations should be started so as to address the legal conflicts that are likely to arise from the fact that many service providers operating on the EU market are based in the US. As highlighted by the European Commission, "[w]hile the e-evidence proposals address the situation of specific types of service providers providing services on the EU market, there is a risk of conflicting obligations with laws in third countries".[918] Indeed, on the one hand, US law prohibits US service providers from disclosing content data to foreign law enforcement authorities[919] (while US-based service providers are allowed to directly cooperate with foreign judicial authorities as regards to non-content data but only on a voluntary, and hence unreliable, basis).[920] On the other hand, the EU legal framework prevents EU service providers from responding directly to requests from foreign authorities, including for non-content data.[921] Negotiations between the EU and the US are hence necessary "so that a transatlantic agreement can be reached on cross-border" – and reciprocal – "access to electronic evidence directly from service providers for use in criminal proceedings".[922] Having regard to this recommendation, in May 2019, the Council gave the European Commission the mandate to negotiate an agreement between the European Union and the United States on facilitating access to e-evidence.[923]

Overall, from the analysis conducted above, it can be concluded that data location as a connecting factor is increasingly losing its relevance in the law enforcement field. The recent developments both at the EU and US levels show that service providers are more and more likely to receive disclosure requests irrespective of the location of the sought-after data. In other words, the transfer of data to third countries does not seem to significantly *increase* the exposure of transferred

[918] European Commission, *Explanatory Memorandum - Recommendation for a Council Decision Authorising 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*, 4.

[919] Ibid.

[920] Ibid., 2.

[921] Ibid., 4.

[922] Ibid., 5.

[923] Council of the European Union, *Council Decision Authorising the Opening of Negotiations with a View to Concluding 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* (Brussels, 2019), accessed December 14, 2019, https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf.

data to disclosure requests issued by foreign public authorities: those data may still be exposed to such requests even if they are stored in the EU, as long as the service provider holding those data is subject to the jurisdiction of a foreign country (in particular of the US under the Cloud Act). Long story short, the "problem of overriding law" – as one on the elements that has so far justified restrictions to international data transfer – is becoming less and less dependent on data location.

As a more general consideration, it seems that, despite its laudable efforts, data protection law cannot by itself solve issues concerning access to data for law enforcement and national security purposes. Assuming or expecting that the EU data protection framework can protect personal data on a global scale by means of the often merely procedural requirements upon which data export restrictions are based is probably an "exalting illusion":[924] national security falls out of the scope of the GDPR[925] (and of EU law more broadly);[926] the Privacy Shield principles can be derogated when it comes to national security and law enforcement concerns; contracts or corporate compliance policies and rules (i.e., appropriate safeguards) are powerless when confronted with data disclosure requests or direct seizure by public authorities;[927] and derogations are inherently incapable of providing any protection, *a fortiori* from access by foreign public authorities.[928] The need to balance security and privacy has certainly come to fore as an issue that needs to be properly addressed. However, the issue of government access to data would probably require the establishment of a set of internationally agreed standards and limitations for surveillance and law enforcement access.[929] Rules on cross-border transfer for commercial purposes do not seem to be the appropriate place for discussing these issues.

[924] Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," 910.

[925] Recital 16 GDPR: "This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security".

[926] Article 4(2), Treaty of the European Union: "...national security remains the sole responsibility of each Member State".

[927] Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," 906–909.

[928] Ibid., 909–910.

[929] For an analysis of the standards for surveillance that have been developed so far and of the possible venues for setting new standards internationally, see Ian Brown, "The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance," *International Journal of Law and Information Technology* 23, no. 1 (2015): 23–40.

5.10. Conclusion

This chapter has set out the architecture of the data transfer mechanisms under the GDPR. The GDPR has essentially endorsed the framework set out under the 1995 Directive together with its structural limitations. A "triumph of bureaucracy and formalism over substance"[930] makes the resort to data transfer restrictions a lengthy and burdensome process, often impractical for SMEs and unsuitable for framing international data transfers when multiple parties and locations are involved. As seen above (5.3), the same restrictions would burden the transfer of data to the United Kingdom as of 1 January 2021 unless an adequacy decision is adopted by the European Commission.

Adequacy decisions are located at the top of the hierarchy of transfer mechanisms. Indeed, under Article 45 GDPR, the transfer of data to a third country or to an international organization may only take place when the European Commission has found the third country or international organization in question to provide an adequate level of protection and, hence, a level of protection which is essentially equivalent (and not necessarily identical) to the one guaranteed in the EU. The analysis conducted above has shown that several doubts have been repeatedly expressed by the EDPB, the EDPS, the European Parliament and, in its annual reviews, by the European Commission about the actual adequacy of the level of protection guaranteed by the Privacy Shield which is the major "enabler" of the data flow from the EU to the US. Similar concerns can also be extended to the adequacy decisions which concern other countries. Moreover, the focus on the *territory* of the whitelisted countries makes adequacy decisions ill-suited to regulate transfers in the cloud where data are transferred and processed in different geographical locations. To make things worse, the process to determine adequacy is notoriously lengthy and only a few countries have been found adequate so far, which makes the practical relevance of this legal basis fairly limited.

As seen above, in the absence of adequacy decisions, data can be transferred if the controller or processor has provided appropriate safeguards. Appropriate safeguards may be provided by

[930] Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," 911.

contractual solutions, such as standard contractual clauses. These contractual solutions aim to "compensate" for the fact that the data recipient is not subject to a set of rules that guarantee an adequate level of protection. This chapter has shown that, although SCCs are widely used in practice, their practical implementation suffer from some significant limitations: SCCs are generally impractical for complex transactions where multiple parties and countries are involved and SCCs for the transfer of data from EEA processors to non-EEA processors are yet to be adopted. Moreover, the same concerns about access to data for surveillance and/or enforcement purposes that have been expressed with reference to the Privacy Shield can be extended to SCCs. Indeed, contractual solutions inevitably yield to any disclosure requests to which the data recipient may be subject (5.5.1.2). The so-called "problem of overring law" may even lead to the invalidation of SCCs in the reference for a preliminary ruling which is currently pending before the ECJ.

As seen above (5.5.2.), appropriate safeguards may also be provided by means of BCRs. BCRs are certainly an efficient tool for framing international data transfer since they allow to carry out multiple transfers between multiple companies of the same group by means of one single instrument. Moreover, it has been noted that BCRs are more than a data transfer tool since they amount to a truly global data protection policy that the members of a group are required to follow regardless of their country of establishment. However, again, several structural limitations negatively impact on the practical relevance of this mechanism, including the fear that BCRs may be exploited to allow the transfer of data to foreign law enforcement and national security authorities.

Among the new legal bases for transfer that have been introduced by the GDPR, it is worth recalling codes of conduct and certification mechanisms. In particular, it has been noted that codes of conduct may not only serve as an international data transfer tool but also as a medium for promoting and spreading internationally the EU standards for data protection. Certification mechanisms may also significantly boost international data transfer since they allow EEA companies to easily identify non-EEA companies that have been certified as providing appropriate safeguards, and non-EEA companies to "signal" to EEA companies their reliability. Specific guidance on the

practical functioning of these new legal bases for transfer is, however, still missing. Derogations under Article 49 GDPR have also been examined. The analysis of derogations concluded by acknowledging their unsuitability for framing transfer on a large scale. Derogations should, indeed, be interpreted and applied in a manner that preserves their exceptional nature. Moreover, it has been noted that the applicability of data transfer rules to EEA data *processors* not only raises several practical challenges but, under certain circumstances, it even seems inconsistent with the intention of the EU legislators.

The chapter has also shown that the very effectiveness of data transfer rules in achieving their underpinning objectives is questionable. As for the anti-circumvention objective, it can be argued that the implementation of data transfer mechanisms is redundant when data are transferred to non-EEA recipients that are *directly* subject to the GDPR by virtue of its extraterritorial reach. This "redundancy" derives from the fact that when data are transferred to non-EEA data recipients that are caught under the territorial scope of the GDPR, there is no real risk that data will be processed inconsistently with the GDPR. Moreover, data location is losing its relevance in the law enforcement field as a basis for grounding requests to disclose electronic data. Indeed, the Cloud Act adopted in the US has "clarified" that CSPs subject to the US jurisdiction can be compelled by US authorities to produce data in their possession regardless of where those data are stored. The EU is going to the same direction as witnessed by the e-evidence proposal. Moving from this analysis, the next chapter will "test" three different possible solutions to the limitations and ineffectiveness of the existing data transfer regime.

6. Seeking the Path(s) Forwards for Boosting International Data Transfer While Protecting Personal Data

6.1. Introduction

The analysis conducted in the previous chapters has highlighted the limitations of the existing data transfer mechanisms in enabling a smooth international data flow while protecting data from unlawful processing and access by foreign public authorities. Despite the simplifications and the novelties introduced by the GDPR, most of the limitations affecting the 1995 Directive have been inherited by the Regulation. In a data-driven economy where data transfer knows no border, the development of a more flexible data transfer system seems compelling in order to allow companies to harness the power of data while preserving customer's trust. While a complete overhaul of the current framework for international data transfer does not seem a feasible option in the near future, some steps that could be taken to improve the system can be identified. This chapter will hence "test" three different possible solutions or, at least, partial solutions to the limitations of the current framework with a view of selecting the *building blocks* upon which a new data transfer regime could be grounded. Firstly, this chapter will analyse the role that global convergence in the data protection field could play in ensuring a free, yet safe, international data transfer; secondly, the claim that has been advanced by many parties (5.9.1.) that data transfer provisions have been made superfluous by the extra-territorial scope of the GDPR will be examined; thirdly, this chapter will define and explore the principle of accountability, as it has been developed both within and outside the European Union, and the promising role that such principle could play as a vehicle for cross-border data flow.

6.2. Solution 1: Solving Data Transfer Issues by Means of Global Convergence

6.2.1. Scope of the Section

If one of the main objectives underpinning data export restrictions is to avoid the circumvention of the EU data protection standards, there would be no need to restrict international data flow if data are transferred to a country that affords an equivalent or, in using the words of the

ECJ in *Schrems*, an "essentially equivalent" level of protection. The most intuitive solution that would make data transfer restrictions "unnecessary" in protecting data would hence be the harmonization of data protection standards at the international level.[931] After all, the global nature of data processing clashes with the regional/national approach to data protection that has been developed so far: in a context where data constantly flow from one country to another thus colliding with divergent regulatory systems of data protection, the "developments of protection standards and instruments can ... no longer be confined to individual or even regional jurisdictions".[932]

At present there is no legally binding instrument that regulates data protection on a global basis. However, with the increase of international data flow, the need to achieve a universal consensus on a set of "standardized" data protection rules has been called by many parties.[933] In 2005, for example, the Data Protection and Privacy Commissioners assembled in Montreux for their 27th International Conference of Data Protection and Privacy Commissioners (ICDPPC) issued the Montreux Declaration in which they agreed "to c*ollaborate* in particular with the governments and international and supra-national organisations for the *development of a universal convention* for the protection of individuals with regard to the processing of personal data". To this end, they appealed "to the United Nations to *prepare a legal binding instrument* which clearly sets out in detail the *rights to data protection and privacy* as enforceable human rights".[934]

The same appeal to the United Nations was reiterated at the 30th ICDPPC in the "Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection" that was adopted in 2008.[935]

---

[931] Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, 35. See also, Benjamin J. Keele, "Privacy by Deletion: The Need for a Global Data Deletion Principle," *Indiana Journal of Global Legal Studies* 16, no. 1 (2009): 365.

[932] Corien Prins, "Should ICT Regulation Be Undertaken at an International Level?," in *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, ed. Bert-Jaap Koops et al. (T.M.C. Asser Press, 2006), 172.

[933] Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (Oxford: Oxford University Press, 2012), 63.

[934] 27th International Conference of Data Protection and Privacy Commissioners, *Montreux Declaration - The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities* (Montreux, 2005), 3 (italics mine), https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf.

[935] 30th International Conference of Data Protection and Privacy Commissioners, *Resolution on the Urgent Need for Protecting Privacy in a Borderless World, and for Reaching a Joint Proposal for Setting International Standards on*

In the said resolution, the Conference also mandated the establishment of a working group coordinated by the Spanish DPA to draft a "Joint proposal for setting international standards on privacy and personal data protection".[936] In keeping with this mandate, the Spanish Data Protection Authority coordinated the work which ultimately lead to the adoption by the 31st ICDPPC of the "Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data" (the so-called "Madrid Resolution").[937] The aim of the said proposal was to "define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data" while, at the same time, facilitating the "international flows of personal data needed in a globalized world".[938] The need to identify and develop some common principles was also included by the ICDPPC in its 2019-2021 strategic plan as a means to bridge different legal systems and, consequently, as a means to support the smooth flow of data across national borders while preserving and boosting citizens' trust. Interestingly, the ICDPPC has noted that while the achievement of common standards should be the goal in the long-term, improved interoperability is a "desirable shorter-term goal".[939]

Similar calls for global standards can also be found within the EU framework. Back in 1997, at the European Ministerial Conference entitled "Global Information Networks: Realising the Potential", the Ministers from the Member States of the European Union, the Ministers of countries of the European Free Trade Association, and the Ministers of countries of the Central and Eastern Europe and Cyprus agreed "to work together towards global principles on the free flow of information

Privacy and Personal Data Protection (Strasbourg, 2008), accessed June 8, 2019, http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resoltuion-on-the-urgent-need-for-protecting-privacy-in-a-borderless-world.pdf.

[936] Ibid., 3.

[937] 31st International Conference of Data Protection and Privacy Commissioners, *International Standards on the Protection of Personal Data and Privacy* (Madrid, 2009), accessed April 15, 2019, http://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf. (hereafter cited as Madrid Resolution).

[938] Art.1, Madrid Resolution.

[939] 41st International Conference of Data Protection and Privacy Commissioners, *Resolution on the Conference's Strategic Direction (2019-21)* (Tirana, 2019), 7, accessed December 22, 2019, https://privacyconference2019.info/wp-content/uploads/2019/10/Resolution-on-the-Conference-Strategic-Direction-2019-2021-FINAL.pdf.

whilst protecting the fundamental right to privacy and personal and business data, building on the work undertaken by the EU, the Council of Europe, the OECD and the UN".[940]

Twelve years later, in 2009, in their Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, the Article 29 Working Party and the Working Party on Police and Justice called upon the Commission

> [t]o take initiatives towards the further development of international global standards regarding the protection of personal data with a view to promote an international framework for data protection and therefore facilitate transborder data flow while ensuring an adequate level of protection of data subjects. These initiatives should include investigating the feasibility of a binding international framework.[941]

The A29WP and the Working Party on Police and Justice hence stressed the importance of achieving global standards as a means to ensure *continued* protection of personal data while allowing data to flow freely and international agreements seem to be the "appropriate instruments for the protection of personal data in a global context".[942] Moreover, the EU should also "encourage the cooperation between international data protection authorities, for example on a transatlantic level" as a "means to promote" – and, it could be added, as a means to enforce – "data protection outside the EU".[943] Notably, in the absence of global standards, the A29WP and the Working Party on Police and Justice called upon the Commission to encourage the adoption of "data protection legislation providing an adequate level of protection" in non-EU countries thus promoting what will be later called a *de facto* approximation of the laws of different countries (6.2.4.).[944]

The EDPS also shown his optimism about the possibility of achieving global data protection standards and about the role of the GDPR as a clarion call for such standards: his hope "is that, during the period of a generation for which the GDPR is likely to apply, we will have achieved a *common*

---

[940] European Union Ministers, *Global Information Networks: Realising the Potential* (Bonn, 1997), accessed June 9, 2019, http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm.

[941] Article 29 Data Protection Working Party and Working Party on Police and Justice, *The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data (WP168)*, 2009, 10 (paragraph 31), accessed December 26, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf.

[942] Ibid., 11 (paragraph 34).

[943] Ibid., 11 (paragraph 36).

[944] Ibid., 10 (paragraph 31).

standard, a sort of *digital gold standard*, which will accompany globalisation and all the benefits and challenges it poses for individuals and society".[945]

Calls for global and legally binding standards have also been expressed within the private sector. In 2007, Peter Fleischer, Google Global Privacy Counsel, listed several reasons that support the need for adopting global privacy standards. Among others, Peter Fleischer noted that in todays' globalized economy, many companies operate in multiple jurisdictions and, as data crosses different geographical regions, companies are also required to abide by different rules. Moreover, "technological development also contributes to the need for global privacy standards" since, while it increases business's productivity, it also exposes privacy to greater risks. In this context, a *fragmented* approach to the new threats to which data are exposed is bound to be ineffectual: "[c]ountries cannot and will not be able to write effective privacy legislation without global cooperation. And as long as there are no global standards for privacy protection, individuals and businesses will remain at risk as they operate online".[946] Along the same lines, back in 2009, in making recommendations about how the 1995 should (have) be(en) reformed, Microsoft suggested that the regulatory developments in other jurisdictions should be taken into account: "[a]s the patchwork of worldwide data protection laws has become increasingly difficult to navigate, Microsoft has repeatedly called for a comprehensive, workable *global* privacy framework that is consistent, flexible, transparent and *principles-based*".[947]

At the same time, several questions inevitably arise when confronting the possibility of developing global and legally binding standards for regulating data protection: who should set such global standards for data protection and by means of which instrument, and how feasible, or even desirable, is harmonization in a context populated by several and often contrasting legislative as well

[945] Giovanni Buttarelli, "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard," *International Data Privacy Law* 6, no. 2 (2016): 78 (italics mine).

[946] Peter Fleischer, "Call for Global Privacy Standards," *Google Public Policy Blog*, September 14, 2007, accessed May 23, 2019, https://publicpolicy.googleblog.com/2007/09/call-for-global-privacy-standards.html.

[947] Microsoft Corporation, *Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 9 (italics mine).

as cultural approaches to the right to data protection? This section will tackle these questions by exploring the existing binding and non-binding initiatives in the data protection field that have been developed at the international level with the view of identifying the instrument and the forum that holds the potentials for setting global standards for data protection. The focus will be placed on the data protection initiatives that have a global, or nearly-global reach. The initiatives that have been taken at the regional level will instead be excluded from this analysis since different regional developments are more likely to lead to fragmentation rather than to harmonization of the law.[948] At the same time, it should be noted that the EU data protection framework on which the present research is focused is one of the most important and full-fledged regional initiatives in the data protection field. Moreover, the developments in cross-border data transfer within the Asia-Pacific Economic Cooperation (APEC) will be examined in section 6.4.[949] The analysis of the initiatives that have been "formally" undertaken at the international level in order to boost data protection will then be followed by an analysis of the *de facto* expansion of the European standards across the globe.

6.2.2. The Right to Data Protection at the International Level

6.2.2.1. United Nations

Certainly, even in the absence of a global privacy treaty, the right to privacy is well and deeply established in the UN legal framework. The first, although non-binding, international instrument that has laid out the right of individuals not to be subjected to arbitrary interference with their private sphere is the Universal Declaration of Human Rights, which in its Article 12 provides that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence ...".[950]

[948] United Nations Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 32; Christopher Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," *Computer Law & Security Review* 25, no. 4 (2009): 313.

[949] Other regional initiatives will be excluded from the analysis (e.g., the data protection framework established by the Association of South East Asian Nations, ASEAN; the African Union Convention on Cyber-security and Personal Data Protection; the Economic Community of West African States Act, ECOWAS; the Commonwealth initiatives; the initiatives within the Organization of American States, OAS, and within the Caribbean Community, CARICOM).

[950] Article 12, United Nations General Assembly, *Universal Declaration of Human Rights*, 1948.

The right to privacy is also enshrined in Article 17 of the 1966 International Covenant on Civil & Political Rights (ICCPR) which provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" and that "[e]veryone has the right to the protection of the law against such interference or attacks".[951] Thanks to its binding nature and the fact that 173 countries are now parties to the Convention, Article 17 ICCPR is the "world's most widely adopted privacy obligation".[952] On the other hand, however, it clearly lacks any details needed for framing global data protection standards.[953]

Moreover, in 1990, the UN General Assembly has adopted its Guidelines for the Regulation of Computerized Personal Data Files.[954] In this document, the General Assembly recommended the adoption of some minimum guarantees that should be provided in national legislations concerning computerized personal data files, among which the principle of lawfulness and fairness in the collection and in the processing of personal data, the principle of accuracy, the principle of purpose-specification and the principle concerning transborder data flows. This latter principle provides that "[w]hen 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".[955]

Following the Snowden revelations about the mass surveillance activities conducted by some States, the UN General Assembly passed two resolutions on the right to privacy in the digital age, the first one in 2013[956] and the second one in 2014.[957] In these resolutions, the General Assembly

[951] Article 17, United Nations General Assembly, *International Covenant on Civil and Political Rights*, 1966.

[952] Graham Greenleaf, *The UN Special Rapporteur: Advancing a Global Privacy Treaty?* (UNSW Law Research Paper No. 2015-69, 2015), 1, accessed May 17, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2672549&download=yes##.

[953] Ibid., 3.

[954] United Nations General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 1990.

[955] Principle 9, ibid.

[956] United Nations General Assembly, *Resolution on the Right to Privacy in the Digital Age* (A/RES/68/167, 2013).

[957] United Nations General Assembly, *Revised Draft Resolution on the Right to Privacy in the Digital Age* (A/C.3/69/L.26/Rev.1, 2014).

expressed its deep concern about "the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, ..., may have on the exercise and enjoyment of human rights";[958] it called upon all States to take measures to stop and to prevent such violations to the right to privacy[959] and to provide individuals with effective remedy in the event that their rights are violated by means of arbitrary surveillance.[960] Moreover, the UN General Assembly encouraged the Human Rights Council to identify and clarify "principles, standards and best practices regarding the promotion and protection of the right to privacy".[961] Even though these resolutions are not legally binding, they have the merit of having triggered a debate at the international level about the implications of new technologies and surveillance activities for the right to privacy.[962]

In 2015, the UN Human Rights Council appointed Prof. Joseph Cannataci as the first ever Special Rapporteur on the Right to Privacy. The Special Rapporteur is mandated, among others, to "gather relevant information, including on international and national frameworks, national practices and experience, to study trends, developments and challenges in relation to the right to privacy and to make recommendations to ensure its promotion and protection, including in connection with the challenges arising from new technologies"[963] and to "identify possible obstacles to the promotion and protection of the right to privacy, to *identify, exchange and promote principles and best practices at the national, regional and international levels*, and to submit proposals and recommendations to the Human Rights Council in that regard, including with a view to particular challenges arising in the digital age".[964] The Special Rapporteur seems hence to be well-equipped for contributing to the

[958] United Nations General Assembly, *A/RES/68/167*, 2.
[959] Ibid.
[960] United Nations General Assembly, *A/C.3/69/L.26/Rev.1*, 4.
[961] Ibid.
[962] European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor, *Handbook on European Data Protection Law*, 2018, 22, accessed May 17, 2019, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.
[963] United Nations Human Rights Council, *The Right to Privacy in the Digital Age* (A/HRC/28/L.27, 2015), 3.
[964] Ibid., 4 (italics mine).

development of global data privacy standards since it is tasked, in particular, with identifying and promoting "principles and best practices at the national, regional and international levels".

It should also be noted that, while the earlier resolutions show that most of the attention at the UN level has been absorbed by the impact of mass surveillance on the right to privacy after the Snowden's revelations, the resolutions adopted in 2016[965] and 2017[966] focus not only on the States' responsibilities in constraining arbitrary access to data by public authorities but also on the responsibility of the private sector in protecting individuals' rights when collecting and processing personal data for their business purposes.[967] In its 2016 resolution, for example, while recognizing "the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms", the UN General Assembly noted that "the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age".[968] To prevent these risks, the UN General Assembly called upon business enterprises to "meet their responsibility to respect human rights"[969] and to "inform users about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency policies, as appropriate".[970] In the same vein, in 2017, the Human Rights Council encouraged business enterprises "to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity, and calls upon States not to interfere with the use of such technical solutions".[971]

[965] United Nations General Assembly, *Revised Draft Resolution on the Right to Privacy in the Digital Age* (A/C.3/71/L.39/Rev.1, 2016).

[966] United Nations Human Rights Council, *The Right to Privacy in the Digital Age* (A/HRC/34/L.7/Rev.1, 2017).

[967] European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor, *Handbook on European Data Protection Law*, 22.

[968] United Nations General Assembly, *A/C.3/71/L.39/Rev.1*, 4.

[969] Ibid., 6.

[970] Ibid.

[971] United Nations Human Rights Council, *A/HRC/34/L.7/Rev.1*, 5.

6.2.2.2. The Organisation for Economic Co-operation and Development

Another initiative that has been taken at the international level in the promotion of privacy as a fundamental value is represented by the adoption by the OECD of its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Guidelines were first adopted in 1980 and were then revised in 2013. The aim of the Guidelines is to "help to harmonise national privacy legislation and, while upholding such human rights, ... at the same time prevent interruptions in international flows of data". To achieve this aim, the Guidelines set out some "basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it".[972]

The eight "basic principles" laid out under the 1980 Guidelines (i.e., collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability) remained unchanged under the revised 2013 version while other parts of the Guidelines have been updated. For example, a new section on accountability has been introduced (Part III on "Implementing Accountability") and the section on transborder data transfer has been updated.[973] Two main themes have guided the revision process: the focus on the practical implementation of the principles on the basis of an approach grounded in risk management, and the need to enhance interoperability as a means to bridge the differences between privacy frameworks.[974]

It should also be noted that the 1980 OECD Guidelines are not limited to the 36 OECD members but they can be followed by any country.[975] Its principles are so widely accepted that they "form the backbone of the principles included in most national privacy laws",[976] including in the legislation of non-European countries, such as Japan, Australia, New Zealand, Canada and Hong

[972] Preface, 1980 OECD Guidelines.

[973] United Nations Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 26.

[974] Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 4.

[975] Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey* (UNSW Law Research Paper No. 17-45, 2017), 6, accessed May 29, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035.

[976] United Nations Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 26.

Kong.[977] At the same time, however, the OECD Guidelines seem to be an unsuitable instrument for setting global data protection standards. One of the major limitations is their non-binding nature. The adherence to the Guidelines is, indeed, voluntary, which does not respond to the need for a *binding* international data protection instrument. Moreover, even in their 2013 "updated" version, the Guidelines embody standards that tend to be lower than the standards that most countries have adopted at the national level:[978] "[t]he current global standard for data privacy laws is closer to the standards of the EU Directive and of Convention 108 than it is to those of the OECD Guidelines".[979]

6.2.2.3. The Council of Europe

The Council of Europe has also played an essential role in promoting the right to privacy. First and foremost, the right to respect for private and family life is laid out under Article 8 of the European Convention on Human Rights.[980] The European Court of Human Rights has examined several cases concerning interferences with this right by both the private sector and public authorities and, in particular, the delicate balance to be struck between the right to respect for private life and other competing rights, like freedom of expression and access to information.[981]

Most importantly, as seen above (4.2.1.), in 1981, the Council of Europe has adopted Convention 108, which is the first *binding* international instrument in the data protection field. Notably, the Convention covers not only the private sector but also the public sector,[982] including the

[977] Lee A. Bygrave, "International Agreements to Protect Personal Data," in *Global Privacy Protection: The First Generation*, ed. James B. Rule and Graham Greenleaf (Cheltenham: Edward Elgar, 2008), 28. For an overview of the countries that have been influenced by the OECD Guidelines in shaping their national data protection laws, see Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 77–79.

[978] Greenleaf, *The UN Special Rapporteur: Advancing a Global Privacy Treaty?*, 3.

[979] Graham Greenleaf, *The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy* (UNSW Law Research Paper No. 18-24, 2018), 2, accessed May 22, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3159846.

[980] Council of Europe, *European Convention on Human Rights* (CETS No. 005, 1950).

[981] European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor, *Handbook on European Data Protection Law*, 23–24.

[982] Under Article 3 of Convention 108, "[t]he Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors".

processing of personal data by law enforcement and judicial authorities[983] which is instead excluded from the scope of the GDPR as it was excluded from the 1995 Directive. The Convention lays out several guarantees in relation to the processing of personal data; it outlaws the processing of sensitive data unless appropriate safeguards are provided by domestic law; it regulates cross-border data flow; and it leaves room for restriction to the rights provided under the Convention in the name of other competing interests, such as State security and public safety.

The guarantees provided under Convention 108 were further improved in 2001 with the adoption of an Additional Protocol which, in line with the 1995 Directive, prescribes the mandatory establishment of one or more supervisory authority by the Parties to the Convention as a means to ensure the effective implementation of the principles of the Convention.[984] To further strengthen the alignment with the 1995 Directive, the Additional Protocol also included provisions about the international data flow to non-Parties to the Convention under which each Party to the Convention "shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer".[985]

The principles laid out under the Convention were further strengthened in the course of the seven-year-long modernisation process of the Convention that was finalised in 2018 (Convention 108 +) with the adoption of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which starting from October 2018 is open for signature.[986] The modernisation of Convention 108 was aimed at addressing the challenges raised by the development of new information and communication technologies and to strengthen the effective

[983] European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor, *Handbook on European Data Protection Law*, 24. See, Council of Europe and Committee of Ministers, *Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector*, 1987.

[984] Article 1, Additional Protocol to Convention 108.

[985] Article 2, Additional Protocol to Convention 108.

[986] On the relationship between Convention 108 and Convention 108 +, see Graham Greenleaf, *'Modernised' Data Protection Convention 108 and the GDPR* (UNSW Law Research Paper No. 19-3, 2018), accessed May 22, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3279984.

implementation of the Convention. In order to achieve these objectives, some of the original principles have been reaffirmed, some have been strengthened, and some new principles and safeguards have been integrated in the modernised version of the Convention.[987] Among the new rights that have been granted to data subjects, it is worth recalling that under Convention 108 +, data subjects are entitled to obtain knowledge of the reasoning underpinning the data processing concerning them;[988] they have the right "not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration";[989] and they have the right "to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms".[990]

Additional obligations are also imposed on those processing personal data: the accountability principle is now fully integrated in the protective scheme laid out under Convention 108 + which burdens data controllers with the obligation to "take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, ..., in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention".[991] Convention 108 + also stresses the importance of the effective implementation of the Convention. Under Article 4 of Convention 108 +, indeed, not only are the Parties required to take the necessary measures in their domestic law to give effect to the provisions under the Convention but a follow-up procedure has also been established to assess the *effectiveness* of such measures.[992] Convention 108 + also recognizes the central role played by

[987] For an overview of novelties adopted under the modernised Convention see, Council of Europe, *The Modernised Convention 108: Novelties in a Nutshell*, n.d., accessed May 20, 2019, https://rm.coe.int/16808accf8.

[988] Article 9(1)(c), Convention 108 +.

[989] Article 9(1)(a), Convention 108 +.

[990] Article 9(1)(d), Convention 108 +.

[991] Article 10, Convention 108 +.

[992] Article 4, Convention 108 +. On this point, see Graham Greenleaf, *International Data Privacy Agreements after the GDPR and Schrems* (UNSW Law Research Paper No. 2016-29, 2016), 3, accessed May 31, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764864.

supervisory authorities in ensuring compliance with the provisions of the Convention. Indeed, the Convention underlines the need to entrust supervisory authorities with effective powers, such as powers of investigation and intervention, the power to issue decisions with respect to violations of the Convention and to impose administrative sanctions.[993]

Most importantly, Convention 108 seems to be the *existing* international legal instrument that is best suited for being elevated to a global data protection agreement. Several elements make Convention 108 a good starting point for globalization. Firstly, its *binding* nature makes it suitable for achieving a great degree of harmonization of the laws of different countries. Convention 108, indeed, offers a *single* text which is legally binding for the States that agree to ratify it, although full harmonization is unlikely since it is not self-executing but it requires Parties to take the necessary steps to implement the principles laid out under the Convention in their domestic legislations. Moreover, as a further obstacle to full harmonization, it allows Parties to derogate from the principles[994] laid out under the Convention in some significant areas.[995]

Secondly, adherence to the Convention is open to any, also non-European countries. It currently counts 55 States:[996] the 47 States that are party to the Council of Europe, plus Argentina, Cap Verde, Mauritius, Mexico, Morocco, Senegal, Uruguay and Tunisia. In addition, the representatives of other States, including Australia, Brazil, Canada, Chile, Gabon, Ghana, Indonesia, Israel, Japan, New Zealand, South Korea, and USA are parties to the Convention Committee as observers.[997]

---

[993] Article 15, Convention 108 +.

[994] Article 9 Convention 108; Article 11, Convention 108 +.

[995] Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," 311–312.

[996] The list of the countries that have ratified Convention 108 is available at this link: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=2fxymMQh. Greenleaf examined the data privacy laws of the 121 countries that, as of mid-2017, had implemented data protection bills with the view of identifying which ones are more likely to meet the requirements for acceding to Convention 108 and concluded that "in addition to the 55 countries already Parties to Convention 108, there are a further 25 non-European countries that could possibly accede to both Convention 108 and to its Additional Protocol (the Council of Europe's preferred course), giving a (very optimistic) maximum of 80". Graham Greenleaf, *Data Protection Convention 108 Accession Eligibility: 80 Parties Now Possible*, 2017, 6, accessed May 30, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062415.

[997] The list of observers as of March 2020 is available at this link: https://rm.coe.int/list-of-observers-nov-2018-en/1680938538.

Thirdly, Convention 108 has inspired the legislative processes in the data protection field in several parts of world, first and foremost, the EU data protection framework. Indeed, the 1995 Directive was built on the basis of the principles included in Convention 108. At the same time, the 1995 Directive has expanded and strengthened those principles,[998] thus making Convention 108 a "moderate version of 'European' standards".[999] The consistency with the EU framework has also been preserved with the modernization of the Convention and the contemporary reform of the EU data protection rules that lead to the adoption of the GDPR.[1000] Indeed, several elements included in the GDPR are also enshrined in Convention 108 + (e.g., proportionality and transparency in data processing, data protection by design and by default) although some other principles set out under the GDPR (e.g., the extraterritorial scope of the rules, right to erasure, obligation to appoint a local representative for foreign controllers or processors) are excluded from Convention 108 +[1001] which, again, makes Convention 108 + a sort of "GDPR Lite".[1002] Besides influencing each other, the standards set out under Convention 108 and the 1995 Directive ("European standards") have *jointly* become global standards since they have inspired the legislative process of many countries throughout the world (6.2.4.).[1003] This entails that the principles established under Convention 108 are consistent with the national legal traditions of many countries which makes the Convention a

[998] European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor, *Handbook on European Data Protection Law*, 29.

[999] Greenleaf, *The UN Special Rapporteur: Advancing a Global Privacy Treaty?*, 3.

[1000] European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor, *Handbook on European Data Protection Law*, 26.

[1001] Graham Greenleaf, *Convention 108+ and the Data Protection Framework of the EU* (UNSW Law Research Paper No. 18-39, 2018), 3–4, accessed May 22, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202606.

[1002] Greenleaf, *The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy*, 2. "When both the GDPR and the modernised Convention 108 are in effect, the new Convention 108 accession standards will be higher, but will still be less demanding than those of the GDPR: 'not too hot, not too cold', a moderate global standard". Graham Greenleaf, *Renewing Data Protection Convention 108: The COE's 'GDPR Lite' Initiatives* (UNSW Law Research Paper No. 17-3, 2016), 4, accessed May 30, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2892947.

[1003] Greenleaf, *The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy*, 1–2. Back in 2013, Greenleaf noted that if the modernization of Convention 108 is conducted consistently with the development of the GDPR (as, indeed, it is the case), "then these two instruments will together constitute a new 'European standard' to replace the current standard created jointly by the EU Directive and the current Convention 108 (and Additional Protocol), which has had a dominant effect on the development of national data protection laws around the globe". Graham Greenleaf, "'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?," *Computer Law & Security Review* 29, no. 4 (2013): 436.

"realistic and desirable" option for building a global data protection agreement. An international agreement should, in fact, mirror the standards that have already gained a certain degree of consensus across the globe.[1004]

Fourthly, Convention 108 specifically addresses enforcement issues by prescribing the appointment of one or more supervisory authorities. This seems to address Moerel's argument (2012) that the adoption of global standards should not be taken as "the holy grail for all international jurisdiction and enforcement issues as presently seen in the data protection field".[1005] Indeed, Moerel argued that even if global standards are established, "differences in enforcement between countries will remain as in practice regulatory enforcement at the national level proves patchy, whether this is due to lack of resources or the prioritization by national governments of national commercial or other interests above regulatory enforcement".[1006] In other words, according to Moerel, any global data protection treaty would have slim chances of having a real bite.[1007] Mattoo and Meltzer (2018) advanced a similar argument when they noted that in order to make sure that data protection rules are enforced once data are transferred to third countries, the regulators in one country would need to influence the behaviour of entities located in other countries. However, "the regulators in other jurisdictions who have control over these entities are not mandated to look out for the interests of citizens from other countries". This entails that even if the harmonization of the data protection rules across different countries is achieved, it would be insufficient to ensure international data flow because of these likely gaps in enforcement.[1008]

[1004] Greenleaf, *The UN Special Rapporteur: Advancing a Global Privacy Treaty?*, 4.

[1005] Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 10.

[1006] Ibid. On the differences in privacy law enforcement in various countries (as for the authorities responsible for enforcing privacy laws, complaint handling, powers of conducting investigations, audits and inspections, sanctions and remedies), see Organisation for Economic Cooperation and Development, *Report on the Cross-Border Enforcement of Privacy Laws*, 12–18.

[1007] Moerel noted that enforcement, both in national and cross-border cases, is made even more problematic by the fact that many companies see the threat of penalties as potential business costs rather than as a deterrent. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 66n25.

[1008] Mattoo Aaditya and Meltzer Joshua P., *International Data Flows and Privacy. The Conflict and Its Resolution*, 2018, 5, http://documents.worldbank.org/curated/en/751621525705087132/pdf/WPS8431.pdf.

Notably, similar concerns about the difficulties in ensuring the enforcement of data protection rules once data are transferred outside the EU have also been expressed by the A29WP with reference to Convention 108 back in 1998 (WP12), and hence before the adoption of the 2001 Additional Protocol, and, of course, before the modernization of the Convention. Indeed, in WP12, the A29WP stressed the importance of assessing the adequacy of the level of protection afforded by a third country on the basis not only of the *content* of the rules applicable to the processing of the transferred data but also of the means for ensuring their effective application (5.4.1.). This "double" requirement derives from the fact that "[o]utside the Community it is less common to find ... procedural means for ensuring compliance with data protection rules". In this regard, the A29WP mentioned that, for example, "Parties to Convention 108 are required to embody the principles of data protection in law, but there is no requirement for additional mechanisms such as a supervisory authority".[1009]

Such pressing enforcement issues have been taken into consideration within the framework set out by Convention 108 which, as seen above, in 2001 was complemented with additional rules on independent supervision (2001 Additional Protocol to the Convention). Following the modernisation of Convention 108, these provisions about the role and the powers of national supervisory authorities are no longer applicable since they have been updated and integrated in the modernized text of Convention 108 +. This should be considered as a positive development since, by acceding to Convention 108 +, countries will also need to abide by the provisions regarding the appointment of a supervisory authority. On the contrary, accession to the Additional Protocol is independent of accession to the Convention so that some countries might only accede to the Convention and not to the Additional Protocol.[1010] Moreover, as it will be discussed below (6.3.4.), Convention 108, in both its "old" and modernized version also includes a section on cross-border cooperation and mutual

[1009] Article 29 Data Protection Working Party, *WP12*, 5, 8.

[1010] Greenleaf, *Data Protection Convention 108 Accession Eligibility: 80 Parties Now Possible*, 2. The Chart of signatures and ratifications of the 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 is available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181/signatures?p_auth=eEKIdKNn.

assistance between supervisory authorities of different countries which aim to ensure the effective implementation of the Convention in cross-border cases.

The idea of Convention 108 as the only *existing* international instrument that has any practical prospects of being developed as a global data protection treaty has been strongly advanced in several occasions by Greenleaf, who noted not only that the adoption of "a new UN data privacy Treaty from scratch is very unlikely" but also that, even if adopted, it "would be likely to have low standards from the outset if it required a consensus of major UN members".[1011] Simply put, Convention 108 "has no realistic competitors as a global privacy instrument".[1012] This idea was strongly advanced by Greenleaf in his submission to a call for inputs on the challenges relating to the right to privacy in the digital age that was launched by the Office of the High Commissioner for Human Rights in 2018:[1013]

> Convention 108 is the only global data protection convention that has any practical prospects of being developed and adopted. The development of a new UN convention from scratch is an unrealistic illusion: agreement on the terms of a new convention would take many years, and could perhaps never be achieved; and even once its terms were agreed, it would take decades to achieve 56 ratifications from across the globe. In contrast, the standards of Convention 108, and its ratifications, have been developing for nearly 40 years. My conclusion, therefore, is that maximizing the opportunities presented by Convention 108 is the UN's best option.[1014]

Greenleaf hence suggested that, instead of developing a new convention from scratch, the UN should align its policies with Convention 108, for example, by recognizing that the standards embodied in Convention 108 have acquired the status of "international 'best practice'" and by encouraging the UN Member States to accede to Convention 108.[1015]

[1011] Greenleaf, *The UN Special Rapporteur: Advancing a Global Privacy Treaty?*, 4. See also Graham Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108," *International Data Privacy Law* 2, no. 2 (2012): 90.

[1012] Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108," 91. Or better, according to Greenleaf, "[t]he most likely alternative is the global order imposed by the economic dominance of Google, Facebook, and other US-based companies, the imperatives of the US economy, and a legal framework which imposes few restraints upon them because of the lack of consistent implementation of most key principles of data privacy protection". Ibid., 92.

[1013] UN Human Rights Council, "Call for inputs to a report on 'the right to privacy in the digital age'", available at https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportPrivacy.aspx.

[1014] Greenleaf, *The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy*, 3.

[1015] Ibid., 3–4.

Notably, these suggestions by Greenleaf seem to have been taken into consideration at the UN level since the ratification of Convention 108 + was encouraged by the Special Rapporteur on the Right to Privacy in his 2018 annual report to the General Assembly of the United Nations. A section of his report is, indeed, devoted to the "[i]ntroduction of privacy and data protection legislation globally". In this section, the Special Rapporteur noted that several important steps in advancing data protection have been taken in 2018 at various levels: at the national level, where an increasing number of countries have passed data protection laws; at the regional level, especially in the EU, where the GDPR came into force; and at the international level, where the modernisation of Convention 108 was finalised.[1016] Against this background, the Special Rapporteur stressed the need to continue the work on the development of international data protection standards,[1017] and that any such development should, as far as possible, be based on international agreements that are regarded as "best practices" in the data protection field and, at the present, these best practices are represented by the GDPR and Convention 108 +.[1018]

In the light of this, the Special Rapporteur considered that commencing work on stand-alone principles would be "premature" since sufficient time should be left in order to assess the robustness of the GDPR and of Convention 108 +.[1019] This is why, his recommendation is that

> [a]s an interim minimum response to agreeing to detailed privacy rules harmonised at the global level, *Member States be encouraged to ratify data protection Convention 108+* ... and implement the principles contained there through domestic law without undue delay, paying particular attention to immediately implementing those provisions requiring safeguards for personal data collected for surveillance and other national security purposes.[1020]

Moreover, in order to ensure a better "alignment of best practices", when transposing Convention 108 + in domestic laws, Member States should also incorporate safeguards laid out under the GDPR but which are not mandatory under the Convention.[1021]

[1016] United Nations General Assembly, *Report of the Special Rapporteur on the Right to Privacy* (A/73/45712, 2018), paragraphs 43-50.
[1017] Ibid., paragraph 117(c).
[1018] Ibid., paragraph 98.
[1019] Ibid., paragraph 101.
[1020] Ibid., paragraph 117(e) (italics mine).
[1021] Ibid., paragraph 117(f).

6.2.2.4. Other Possible International Fora for the Creation of Global Data Protection Standards

In the absence at the international level of a body specifically mandated with the task of leading the work on the drafting of an international data protection treaty, several *existing* bodies have been named as possible fora for the setting of international data protection standards. The International Law Commission (ILC), which has "for its object the promotion of the progressive development of international law and its codification",[1022] has been mentioned as a possible body which could coordinate the preparation of an international convention on data protection. The ILC has, indeed, included in its long-term programme of work the "Protection of personal data in the transborder flow of information",[1023] which may lead to the preparation of a binding international convention on data protection.[1024] However, the inclusion of a topic in the long-term program of work of the ILC does not automatically entail that the topic will become a specific subject of its work. A separate decision by the ILC would, indeed, be necessary to that effect.[1025] The United Nations Educational, Scientific and Cultural Organization (UNESCO) and the International Telecommunications Union have also been named as possible focal points for the preparation of global data protection rules. However, these bodies are specialized agencies which makes them unfit for triggering discussion in such a multi-faceted area like data protection[1026] which is "a mixture of various legal areas, such as human rights law, public law, private law, and others".[1027]

Moreover, considering the close connections between data flow and trade, another option could be to entrust the World Trade Organization (WTO) with the task of leading the work on the preparation of global data protection rules. At the same time, however, despite the strong economic reasons underpinning calls for free flow, its focus on open trade and economic growth makes the

[1022] Article 1(1), *Statute of the International Law Commission*, 1947.

[1023] United Nations General Assembly, *Report of the International Law Commission Fifty-Eighth Session (1 May-9 June and 3 July-11 August 2006* (A/61/10, 2006).

[1024] Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," 308.

[1025] See the International Law Commission website: https://legal.un.org/ilc/programme.shtml.

[1026] Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," 312.

[1027] Ibid., 315. See also, Philipp E. Fischer, "Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 3, no. 1 (May 15, 2012): 48, accessed June 10, 2019, http://www.jipitec.eu/issues/jipitec-3-1-2012/3321.

WTO ill-equipped for dealing with data protection as a basic human right.[1028] Indeed, in several occasions, the European Commission has made clear that "dialogues on data protection and trade negotiations with third countries have to follow separate tracks"[1029] since privacy is not a commodity that can be negotiated in trade agreements.[1030] Not by chance, back in 2013, after Snowden's revelations, the European Commission made clear that data protection standards were not going to be included in the negotiations (which were launched in 2013 and ended in 2016 without conclusion) with the US on the Transatlantic Trade and Investment Partnership (TTIP).[1031] This decision derives from the consideration that, as warned by Viviane Reding, Vice-President of the European Commission, "[d]ata protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable".[1032]

At the same time, while data protection standards shall be excluded from trade negotiations, the European Commission has stressed that trade rules can be used to contrast unjustified data localization requirements as a form of digital protectionism and not as a form of data protection. Indeed, in its 2015 trade and investment strategy, besides committing to ensure that data protection

[1028] Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," 312. On the contrary, according to Reidenberg (2000), the WTO could be a suitable launching point for a "Global Agreement on Information Privacy" (GAIP). Indeed, although "the WTO has an inherent bias toward liberal, market norms ... the breadth of membership in WTO and the growing recognition at WTO that social values such as workers' rights and environmental issues are intrinsically linked to trade will blend governance ideologies. Noneconomic values will bring non-market based governance norms to WTO ... The WTO accords expressly recognize privacy as a value that can override the free flow of information principle enshrined in the annex agreement on services. The significance of putting GAIP before the WTO is, thus, twofold. First, the WTO framework offers an institutional process with wide membership. Second, while the institution leans toward market-based norms, the incorporation of GAIP within the WTO along with other noneconomic values will transplant social- protection norms to the trade arena. In effect, this transplantation will promote convergence of governance norms". Joel R. Reidenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace," *Stanford Law Review* 52, no. 5 (2000): 1361–1362, accessed February 7, 2018, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1040&context=faculty_scholarship.

[1029] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. "Building A European Data Economy,"* COM(2017) 9 final. (Brussels, 2017), 4, accessed June 5, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN.

[1030] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 6.

[1031] European Commission - Press release, "European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows," last modified November 27, 2013, accessed June 7, 2019, http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

[1032] European Commission - Press release, "Towards a More Dynamic Transatlantic Area of Growth and Investment," last modified October 29, 2013, accessed June 7, 2019, http://europa.eu/rapid/press-release_SPEECH-13-867_en.htm?locale=en.

rules will not be negotiated in trade agreements,[1033] the European Commission also stated that the "goal for the EU should be the creation of a global level playing field, with non-discrimination and the absence of unjustified data localisation requirements". In pursuit of this goal, the European Commission will seek to use free trade agreements to "tackle new forms of digital protectionism, in full compliance with and without prejudice to the EU's data protection and data privacy rules".[1034]

The European Commission further clarified its position on the relationship between data protection and external trade policy in its 2017 Communication on "Exchanging and Protecting Personal Data in a Globalised World" in which it reiterated that data protection rules cannot be subject to negotiations in free trade agreements. Rather, dialogues on data protection with third countries in order to ensure "uninhibited flow of personal data" should take the form of adequacy decisions. Adequacy findings are hence the best avenue to facilitate commercial exchanges with third countries involving personal data. Such decisions may therefore "complement existing trade agreements, thus allowing them to amplify their benefits" while, at the same time, fostering convergence of the level of protection guaranteed in third countries.[1035] Interestingly, the European Commission also recognized the role that adequacy decisions may play in contrasting unjustified data localization requirements: "by fostering the convergence of the level of protection in the EU and the third country, an adequacy finding reduces the risk of invocation by that country of personal data protection grounds to impose unjustified data localisation or storage requirements".[1036]

The European Commission's approach of excluding data protection from trade negotiations is also supported by the Council of the European Union: the "Council stresses the need to create a global level playing field in the area of digital trade and strongly supports the Commission's intention to pursue this goal in full compliance with and without prejudice to the EU's data protection and data

[1033] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Trade for All Towards a More Responsible Trade and Investment Policy*, COM(2015) 497 final. (Brussels, 2015), paragraph 2.1.2, accessed June 5, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0497&from=ga.

[1034] Ibid.

[1035] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 9.

[1036] Ibid.

privacy rules, which are not negotiated in or affected by trade agreements".[1037] Along the same lines, in its resolution of 3 February 2016 containing the recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA),[1038] the European Parliament stressed that "data protection is not an economic burden, but a source of economic growth" and that trade in services "should never compromise the EU's *acquis* on data protection and the right to privacy".[1039] The European Parliament hence recommended the European Commission to ensure "cross-border data flows in compliance with the universal right to privacy",[1040] "to incorporate a comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV[1041] which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement";[1042] and, "to reject, therefore, any 'catch-all' provisions on data flows which are disconnected from any reference to the necessary compliance with data protection standards".[1043] The same position is reflected in the TTIP resolution which was adopted by the European Parliament a year earlier.[1044]

In a letter sent to President Juncker on 15 December 2016, the European Parliament urged the European Commission to "put forward its position on cross-border data flows in trade negotiations". In the said letter, the European Parliament reiterated that trade agreements should not prevent the

---

[1037] Council of the European Union, *3430th Council Meeting, Outcome of the Council Meeting* (Brussels, 2015), paragraph 9, accessed June 7, 2019, http://data.consilium.europa.eu/doc/document/ST-14688-2015-INIT/en/pdf.

[1038] For further information on the TiSA see, http://ec.europa.eu/trade/policy/in-focus/tisa/.

[1039] Recital M, European Parliament, *Resolution of 3 February 2016 Containing the European Parliament's Recommendations to the Commission on the Negotiations for the Trade in Services Agreement (TiSA)* (2015/2233(INI), 2016), accessed January 6, 2019, https://www.europarl.europa.eu/doceo/document/TA-8-2016-0041_EN.pdf.

[1040] Recommendation 1(c)(i), Ibid.

[1041] Article XIV, *General Agreement on Trade in Services, Marrakesh Agreement Establishing the World Trade Organization* (Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167, 1994). "Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, *nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures*: … (c) *necessary to secure compliance with laws or regulations* which are not inconsistent with the provisions of this Agreement including those relating to: ... (ii) 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" (italics mine).

[1042] Recommendation 1(c)(iii), European Parliament, *Resolution of 3 February 2016 Containing the European Parliament's Recommendations to the Commission on the Negotiations for the Trade in Services Agreement (TiSA)*.

[1043] Recommendation 1(c)(iv), Ibid.

[1044] European Parliament, *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))*, 2015, accessed June 28, 2020, https://www.europarl.europa.eu/doceo/document/TA-8-2015-0252_EN.pdf.

European Union from applying and improving its own data protection rules and that data transfer rules should not be "diluted" in the context of trade negotiations. European standards should hence be safeguarded in trade agreements negotiated by the EU: the same standards of protection should be applied both at the domestic and at the international level in order to ensure consumers' trust and legal certainty to businesses. At the same time, the European Parliament acknowledged that data flows "have become the backbone of our economies and the bedrock of international trade" and, for that reason, data flows "should not be unduly prohibited by means of unjustified forced data localisation requirements".[1045]

Most importantly, in its resolution of 12 December 2017 on "Towards a digital trade strategy",[1046] the European Parliament called on the European Commission to draft rules for cross-border data transfer which are fully consistent with the existing EU data protection framework and "to incorporate into the EU's trade agreements a horizontal provision, which fully maintains the right of a party to protect personal data and privacy, provided that such a right is not unjustifiably used to circumvent rules for cross-border data transfers for reasons other than the protection of personal data". Those rules should become part "of all new and recently launched trade negotiations with third countries".[1047] The European Parliament also stressed that unjustified data localisation requirements should be strictly prohibited in free trade agreements and that such requirements should not be used "as a form of non-tariff barrier to trade and as a form of digital protectionism". The removal of those requirements is hence a "top priority".[1048]

In 2018, the European Commission presented its "Horizontal" – meaning that they cover all economic sector – "provisions for cross-border data flows and for personal data protection"[1049] in

[1045] *Letter from MEPs Jan Albrecht, Bernd Lange, Viviane Reding and Marietje Schaake to President Juncker*, 2016, accessed June 28, 2020, https://marietjeschaake.eu/en/data-flows-letter-to-president-juncker.

[1046] European Parliament, *Resolution of 12 December 2017 on "Towards a Digital Trade Strategy"* (2017/2065(INI), 2017), accessed June 28, 2020, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf.

[1047] Ibid., paragraph 11.

[1048] Ibid., paragraph 12.

[1049] European Commission, *Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements)*, 2018, accessed June 28, 2020, https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

trade and investment agreements. Those provisions have been drafted in order to oppose protectionist practices adopted by third countries while also ensuring that the high standards of data protection guaranteed in the EU are not undermined by trade agreements.[1050] Article A of the horizontal provisions on cross-border data flow specifically tackle data localization requirements by prescribing the following:

> The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:
> (i) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;
> (ii) requiring the localisation of data in the Party's territory for storage or processing;
> (iii) prohibiting storage or processing in the territory of the other Party;
> (iv) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.[1051]

This Article hence includes a commitment to ensure cross-border data flows and a prohibition of a list of four types of data localization requirements, list which the Parties may review at any time.

Article A on "cross-border data flows" is then followed by Article B on "protection of personal data and privacy" which aims to ensure that the commitments agreed in the trade agreement do not undermine the level of protection of personal data and privacy afforded by the Parties to the agreement. To this end, each "Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy" – which each Party recognizes as fundamental rights – "*including* through the adoption and application of *rules for the cross-border transfer of personal data*".[1052] A clear line is hence drawn between (unjustified) data localization measures on the one hand and rules for the cross-border data transfer which respond to (justified) privacy concerns on the other.[1053]

[1050] European Commission - Expert Group on Trade Agreements, *Meeting Report of 11 July 2018*, 2018, 4, accessed July 1, 2020, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=15690.

[1051] Article A on "Cross-border data flow", European Commission, *Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements)*.

[1052] Article B on "Protection of personal data and privacy" (italics mine), Ibid.

[1053] For a detailed analysis of EU's external trade policy, see Svetlana Yakovleva and Kristina Irion, "Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade," *International Data Privacy Law* (n.d.): 17–20, accessed June 28, 2020, http://academic.oup.com/idpl/advance-

These provisions could hence serve as the starting point for negotiations of free trade agreements and bilateral investment treaties between the EU and third countries.[1054] The European Commission has already started to implement the said provisions in trade negotiations with third countries. In particular, the formulation presented by the European Commission was submitted in July 2018 in trade negotiations with Indonesia with the specific aim to prohibit protectionist barriers without prejudice to EU data protection standards.[1055] These provisions have also been proposed in negotiations with Australia[1056] and New Zealand[1057] and have been tabled to Chile.[1058]

As for the most recent agreement concluded with Japan, i.e., the EU and Japan's Economic Partnership Agreement[1059] which entered into force on 1 February 2019, Article 8.63 of the said Agreement on "Transfers of information and processing of information" gives the Parties to the Agreement the right to adopt data protection measures as long as that right is not used to circumvent some sections of the Agreement. The free flow of data is addressed in Article 8.81 in the form of a

article/doi/10.1093/idpl/ipaa003/5813832; Federica Velli, "European Papers," *The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements* 4, no. 3 (2019): 881–894, accessed July 1, 2020, http://www.europeanpapers.eu/en/europeanforum/issue-of-data-protection-in-eu-trade-commitments.

[1054] For a detailed analysis of horizontal clauses and of the different approaches underpinning adequacy decisions on the one hand and horizontal clauses on the other, see Gabriele Rugani, "Data Protection Provisions in New Generation Free Trade Agreements: Advantages and Critical Issues," in *"The New Generation of EU FTAs: External and Internal Challenges,"* ed. Isabelle Bosse-Platière, Cécile Rapoport, and Nicolas Pigeon (LAwTTIP Working Papers 2019/6, 2019), 60–74, accessed July 1, 2020, https://www.lawttip.eu/uploads/files/LAwTTIP%20Working%20Paper_2019_6_Event%2013(1).pdf.

[1055] The texts proposed by the EU for the trade deal with Indonesia as a basis for discussion are available at: http://trade.ec.europa.eu/doclib/press/index.cfm?id=1620. See also European Commission, *5th Round of Trade Negotiations between the European Union and Indonesia - EU Provisions on Cross-Border Data Flows and Protection of Personal Data and Privacy in the Digital Trade Title of EU Trade Agreements*, 2018, accessed June 30, 2020, https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf.

[1056] European Commission, *Proposal for the EU-Australia Free Trade Agreement - Digital Trade Title*, 2018, accessed June 30, 2020, https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf.

[1057] European Commission, *EU-New Zealand Free Trade Agreement - Digital Trade Title*, 2018, accessed July 1, 2020, https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf.

[1058] European Commission - Expert Group on Trade Agreements, *Meeting Report of 11 July 2018*, 4. The EU proposal for a Digital trade title in the Trade Part of a possible modernised EU-Chile Association Agreement published on 6 February 2018 includes a placeholder for provisions on data flows and data localization. The EU proposal for a Digital trade title is available at: https://trade.ec.europa.eu/doclib/docs/2018/february/tradoc_156582.pdf. The Report on the 7th round of negotiations between the EU and Chile for the modernisation of the trade part of the EU Chile Association Agreement which took place from 25 to 29 May says that "[t]he parties continued to discuss data flows and personal data protection, as well as exchanging views on the non-discrimination of digital products. Further work is needed in these areas". See, European Commission, *Report on the 7th Round of Negotiations between the EU and Chile for the Modernisation of the Trade Part of the EU Chile Association Agreement*, 2020, 2, accessed June 1, 2020, https://trade.ec.europa.eu/doclib/docs/2020/june/tradoc_158772.pdf.

[1059] The Agreement between the European Union and Japan for an economic partnership is available at: https://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf.

"*rendez-vous*" clause:[1060] the "Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement". As clarified by Ms Malmström on behalf of the European Commission, the reason for the inclusion of this review clause is that "at the time of the political agreement concluded in July 2017 internal Commission discussions on data flows were still ongoing" and the horizontal provisions had not been published yet. Within three years of the entry into force of the Agreement, "the Commission will assess the need to include provisions on data flows and data protection".[1061] Most importantly, the European Commission has reproduced its position in the proposal released by the European Union in April 2019 on new WTO rules for electronic commerce,[1062] which is part of the talks on e-commerce that have been launched by 76 WTO members in the margins of the Davos World Economic Forum in January 2019.[1063]

6.2.3. The Feasibility and the Desirability of International Data Protection Standards

In the light of the framework set out above, the chances of achieving a truly international data protection treaty in the next few years appear slim. Indeed, as seen above, the option of developing a UN-sponsored data protection treaty is considered "premature" even by the UN Special Rapporteur on the right to privacy (6.2.2.3.) and no international body has been specifically entrusted with negotiating an international agreement on privacy issues (6.2.2.4.). Convention 108 is the only *existing* international instrument that has any practical prospects of being developed as a global data protection treaty. However, a true globalisation of the Convention is yet to be achieved and, even if it is achieved, its standards might not be considered "adequate enough" by the EU since the standards

[1060] Yakovleva and Irion, "Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade," 4.

[1061] Parliamentary questions - Answer given by Ms Malmström on behalf of the Commission, available at: https://www.europarl.europa.eu/doceo/document//P-8-2018-002756-ASW_EN.html.

[1062] World Trade Organization, *Joint Statement on Electronic Commerce. EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce. Communication from the European Union* (INF/ECOM/22, 2019), accessed June 5, 2019, http://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

[1063] World Trade Organization, *Joint Statement on Electronic Commerce* (WT/L/1056, 2019), accessed June 5, 2019, http://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf.

included in the Convention are a "moderate version of 'European' standards"[1064] (6.2.2.3.). Questions could also be raised about the level of details that can feasibly be achieved, or that should be achieved when framing an international data protection treaty. Indeed, reaching international consensus on a whole array of details about how data should be processed is hardly realistic. As suggested by Moerel (2012), "[a]ny global standard should ... in any event be limited to setting general principles, leaving any detailed rules to secondary regulation which can be amended more quickly, if changing circumstances so require".[1065]

Another element of complexity should be added to the puzzle: data protection legislation mirrors different cultural values so that bridging differences in privacy legislations would also entail bridging cultural differences.[1066] The most obvious and commented-on example is represented by the opposite approaches adopted in the EU, which has adopted a comprehensive and all-encompassing regulatory model, and in the US, which has preferred, at least so far, a "piecemeal" model in which a number of both federal and state-level regulations tackle privacy issues on a sector-oriented manner.[1067] These differences in the approach to privacy that have been developed in the two regions essentially mirror the different view on the role that the State should play in protecting citizens' rights and on the ability of the market to grant a fair treatment of citizens.

In this regard, it should be recalled that the Unites States has a tradition of distrust towards the government which is reflected in its hostility towards regulation of private relations. US decision makers have emphasized the role of private actors and market forces in addressing societal challenges while the traditional role of the government is to act as a rule maker of last resort which only intervenes when the private sector fails. The US liberal philosophy has hence led to a preference for markets and self-regulation in privacy matters: privacy is seen as a tradable commodity and the free

[1064] Greenleaf, *The UN Special Rapporteur: Advancing a Global Privacy Treaty?*, 3.

[1065] Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 67.

[1066] Bygrave, "International Agreements to Protect Personal Data," 48. See also, Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, 35.

[1067] Cécile de Terwangne, "Is a Global Data Protection Regulatory Model Possible?," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Amsterdam: Springer, 2009), 179–180; Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108," 70–72.

market is seen as the most effective mechanisms for protecting it. On the other hand, European decision makers have always tended to see a wide role for the State and the government in addressing social problems. The State is the necessary player in charge of framing social community and the development of citizen autonomy lies on a background of legal rights. In this framework, privacy is seen as a fundamental human right which cannot be traded away and which the government is responsible for providing to its citizens. Moreover, unlike the United States, some European countries have experienced the atrocities of Nazi-fascist dictatorships (e.g., Italy, Germany, Spain and Austria) and of other repressive regimes (in East Europe) which have sensitized Europeans to the importance of protection against improper use of personal data.[1068]

Moreover, economic considerations also come into play: "national privacy protection can have economic costs ... and the relative importance of these costs can differ across countries".[1069] Developing countries, for example, may strike a different balance compared to EU countries between protection of personal data and the economic potentials that derive from the use of such data. Developing countries may, in fact, value the economic opportunities offered by the Internet more than protection of individuals from the privacy risks that may derive from the Internet. The adoption of data protection rules that meet the high threshold set by the EU standards may hence contrast with this different balance:[1070]

> The standard that is appropriate in an advanced country with well-developed markets and comprehensive access to services is not necessarily appropriate for a poor country. Prematurely stringent privacy laws could hurt the efficiency and development of financial and other markets by inhibiting the flow of information. Enacting such national privacy legislation would increase the economy-wide cost of doing business, which would hurt access to services at home and competitiveness in foreign markets which do not have EU-like privacy regulation.[1071]

[1068] For an analysis of the different approaches developed in the EU and in the US, see, among others, Lauren B. Movius and Nathalie Krup, "U.S. and EU Privacy Policy: Comparison of Regulatory Approaches," *International Journal of Communication* 3 (2009): 169–187, accessed February 7, 2018, http://ijoc.org/index.php/ijoc/article/view/405/305; Reidenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace," 1342–1351; Andreas Busch, "The Regulation of Privacy," *Jerusalem Papers in Regulation & Governance, Working Paper No. 26* (2010): 11, accessed February 7, 2018, http://regulation.huji.ac.il/papers/jp26.pdf.

[1069] Aaditya and Joshua P., *International Data Flows and Privacy. The Conflict and Its Resolution*, 4.

[1070] Ibid., 14.

[1071] Ibid., 28.

An example of the dilemma faced by developing countries when confronting the possibility of adopting GDPR-like data protection rules in order to keep the flow of data from the EU is offered by the Philippines. Indeed, after that the Philippines had adopted high standards of data protection, many US companies based in the Philippines decided to interrupt investment plans due to the difficulties of complying with the new stringent data protection rules.[1072]

6.2.4. The EU Framework as a "Trendsetter" of Data Protection Standards

Despite the presence of different privacy cultures, it should be noted that, as mentioned above (6.2.2.3.), the European standards seem to have had a real grip in non-European countries. The EU framework has, indeed, been defined as the "most prominent trendsetter for data protection norms around the world".[1073] In other words, even in the absence of *direct* international negotiations and implementation of global standards, a certain degree of harmonization has been reached in the data protection field thanks to *indirect* instruments, like regional pressure coming from the EU whose standards have been exported across the globe:[1074] "[a]s more countries joined the data protection 'club' so there was increasing pressure on those outside the club to pass equivalent laws".[1075] As noted by Greenleaf (2016), "[o]utside Europe, a mixture of the influence of perceived 'adequacy' requirements in the GDPR, what is required for Convention 108 accession, and desire to emulate European 'best practices' will be" – and has been – "influential".[1076]

Most of the pressure coming from the EU seems to derive from the use of adequacy decisions which, indeed, often translates into a form of coercion on non-EU countries by making access to some specific resources (i.e., access to data coming from the EU) conditional upon compliance with the EU data protection standards. Kuner (2017) defined the use of adequacy decisions as a "carrot and

[1072] Ibid., 15.
[1073] Bygrave, "International Agreements to Protect Personal Data," 47.
[1074] Prins, "Should ICT Regulation Be Undertaken at an International Level?," 172.
[1075] Colin Bennett, "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?," *Information Polity* 23 (2018): 240, accessed May 28, 2019, https://pdfs.semanticscholar.org/3813/041fc44467933d64c54c3e39a467c2be63c3.pdf.
[1076] Greenleaf, *International Data Privacy Agreements after the GDPR and Schrems*, 5.

stick approach": the carrot is the possibility for third countries to acquire a preferential status and hence maximize the economic benefits underpinning free flow of data from the EU, while the stick is the fact that the EU framework prohibits the flow of data to third countries which do not provide an adequate level of protection.[1077] At the same time, it should be noted that, besides the perceived *economic* advantage of importing data from the EU under an adequacy decision, the influence of EU standards outside the EU seems also to be linked to the *practical* advantage of following an existing and full-fledged data protection system as a template rather than drafting an entirely new piece of legislation.[1078]

In this regard, in order to find evidence of the influence exerted by European standards outside the EU, in 2012, Greenleaf analysed the data privacy laws of 33 non-European countries (out of the 39 laws existing back then outside Europe) with the view of identifying which and how many "European elements" are incorporated in those laws.[1079] The conclusion of his study was the following:

> Although more evidence of causation is desirable, it is an entirely plausible (and in my view, correct) hypothesis that the EU Directive is the most significant overall influence on the content of data privacy laws outside Europe, ... Second, its influence is gradually strengthening, partly because of the desire of non-EU countries to have their laws recognized as 'adequate', but also because of the aspiration that their laws should be recognized as providing the highest international standard of privacy protection.[1080]

In other words, according to Greenleaf, not only is there sufficient evidence of the strong influence exerted by the 1995 Directive in non-European jurisdictions, but such influence is also likely to increase as a means, at least partly, to meet the adequacy standards set out under Article 25 of the 1995 Directive and, now, under Article 45 of the GDPR. The same exercise was repeated by

[1077] Kuner, *The Internet and the Global Reach of EU Law*, 24–25. On this point see also, Agustín Rossi, "Internet Privacy: Who Sets the Global Standard?," *The International Spectator* 49, no. 1 (2014): 69.

[1078] Kuner, *The Internet and the Global Reach of EU Law*, 18.

[1079] Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108," 74–77. In his study, Greenleaf identified ten "European elements", namely the elements that are prescribed under the 1995 Directive and, sometimes, also by Convention 108 but which are not included in the OECD (e.g., requirement of an independent DPA, possibility of recourse to the courts in case of infringement of data protection rights).

[1080] Ibid., 77. Greenleaf found out that all jurisdictions examined except four (Japan, Bahamas, Vietnam, and Chile) share at least four of the ten "European elements". Ibid., 76.

Greenleaf in 2017. This time, however, since by February 2017 the number of non-European data privacy laws had increased from 39 to 66, he limited the comparison to 20 of the "most significant" countries by GDP[1081] and he found that, on average, the data privacy laws of the countries examined contained 5.95 of the ten European standards. He hence concluded that there is strong evidence that European data privacy standards have been adopted to a substantial extent outside Europe.[1082]

The past forty years have, indeed, witnessed a sort of *de facto* convergence with more and more non-European countries adopting or starting the process of adopting privacy laws close to the European standards.[1083] Australia, Hong Kong, South Korea, Dubai, South Africa all passed data protection bills that are modelled on or, at least, that shows influence from the EU data protection legislation.[1084] In August 2018, Brazil also passed a new data protection law (Lei Geral e Única de Proteção de Dados Pessoais or LGPD) that clearly mirrors several provisions under the GDPR. Among others, like the GDPR, LGPD has an extraterritorial application since the duty to comply with the Brazilian law extends beyond its geographical borders; its definition of "personal data" resembles the definition provided under the GDPR; it includes the six legal bases for processing personal data that are provided under the GDPR with the addition of four legal bases (for a total of 10 legal bases); international data transfer is restricted unless an adequacy decision or, in the absence of an adequacy decision, other instruments are in place; moreover, a national data protection authority was set up by the Executive Order n. 869 of 27 December 2018 which brought some changes to the LGPD.[1085]

[1081] Graham Greenleaf, *'European' Data Privacy Standards Implemented in Laws Outside Europe* (UNSW Law Research Paper No. 18-2, 2017), 1–2, accessed May 30, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3096314. The selected countries are: Japan; India; Canada; South Korea; Australia; Mexico; Indonesia; Argentina; Taiwan; Hong Kong; Israel; the Philippines; Malaysia; Singapore; South Africa; Colombia; Chile; Vietnam; Peru; and New Zealand. For an analysis of the expansion of data privacy laws across the globe, see Graham Greenleaf, *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories* (UNSW Law Research Paper No. 2013-40, 2013), accessed May 31, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877.

[1082] Greenleaf, *'European' Data Privacy Standards Implemented in Laws Outside Europe*, 2–3.

[1083] Greenleaf, *The UN Special Rapporteur: Advancing a Global Privacy Treaty?*, 3.

[1084] Bygrave, "International Agreements to Protect Personal Data," 47.

[1085] Angelica Mari, "Brazil Moves Forward with Online Data Protection Efforts," *ZDNet*, last modified July 5, 2018, accessed August 3, 2018, https://www.zdnet.com/article/brazil-moves-forward-with-online-data-protection-efforts/; "What Is the Brazil General Data Protection Law (LGPD)?," *OneTrust*, July 20, 2018, accessed May 24, 2019, https://www.onetrust.com/what-is-the-brazil-general-data-protection-law-lgpd/; Renato Leite Monteiro, "The New Brazilian General Data Protection Law — a Detailed Analysis," *Iapp*, August 15, 2018, accessed May 24, 2019, https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/; Melanie Ramey, "Brazil's

Argentina, which is the first Latin-American country which was found adequate by the European Commission,[1086] is going in the same direction. Indeed, in 2018 the Congress has started to discuss a GDPR-style bill which, if adopted, would replace the current data protection bill. The provisions in the draft bill closely follow the GDPR standards, including a major overhaul of the section on data transfers which, under the proposed bill, can lawfully take place when, for example, contractual clauses are in place or when binding corporate rules have been implemented, or when the data subject has consented to the transfer.[1087] Along the same lines, several GDPR provisions have been followed and replicated in the new Thailand Personal Data Protection Act, i.e., the first comprehensive data protection law adopted in Thailand which was published in the Government Gazette on 27 May 2019.[1088] The same considerations can be extended to Nigeria. Indeed, in January 2019, the National Information Technology Development Agency of Nigeria, "COGNIZANT of emerging data protection regulations within the international community geared towards security of lives and property and fostering the integrity of commerce and industry in the volatile data

New General Data Privacy Law Follows GDPR Provisions," *Inside Privacy*, last modified August 20, 2018, accessed May 24, 2019, https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/; Bruno Bioni, Maria Cecília Oliveira Gomes, and Renato Leite Monteiro, "GDPR Matchup: Brazil's General Data Protection Law," *Iapp*, October 4, 2018, accessed May 24, 2019, https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/; Renato Leite Monteiro, "Changes to Brazil's Data Protection Law and the Establishment of the DPA," *Iapp*, January 3, 2019, accessed May 24, 2019, https://iapp.org/news/a/changes-to-brazils-data-protection-law-and-the-establishment-of-the-dpa/; Isabel Carvalho and Rafael Loureiro, "Brazil Creates a Data Protection Authority," *HL Chronicle of Data Protection*, last modified January 11, 2019, accessed May 24, 2019, https://www.hldataprotection.com/2019/01/articles/international-eu-privacy/brazil-creates-a-data-protection-authority/.

[1086] European Commission, *Commission Decision of 30 June 2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina* (L 168/19, 2003).

[1087] Pablo A. Palazzi and Andres Chomczyk, "GDPR Matchup: Argentina's Draft Data Protection Act," *Iapp*, August 24, 2017, accessed May 29, 2019, https://iapp.org/news/a/gdpr-matchup-argentinas-draft-data-protection-act/; Diego Fernandez, "Argentina's New Bill on Personal Data Protection," *Iapp*, October 2, 2018, accessed May 29, 2019, https://iapp.org/news/a/argentinas-new-bill-on-personal-data-protection/; "Argentina Publishes GDPR-Style Data Protection Bill," *Privacy Laws & Business*, last modified September 24, 2018, accessed May 29, 2019, https://www.privacylaws.com/news/argentina-publishes-gdpr-style-data-protection-bill/; "DPA of Argentina Issues Draft Data Protection Bill," *Privacy & Information Security Law Blog*, February 9, 2017, accessed May 29, 2019, https://www.huntonprivacyblog.com/2017/02/09/dpa-argentina-issues-draft-data-protection-bill/.

[1088] Dhiraphol Suwanprateep, "Get Ready: The First Thailand Personal Data Protection Act Has Been Passed," *Baker McKenzie*, last modified March 1, 2019, accessed June 5, 2019, https://www.bakermckenzie.com/en/insight/publications/2019/03/the-first-thailand-personal-data; Dhiraphol Suwanprateep and Nont Horayangura, "Thailand Personal Data Protection Act," *Baker McKenzie*, last modified May 28, 2019, accessed June 5, 2019, https://www.bakermckenzie.com/en/insight/publications/2019/05/thailand-personal-data-protection-act; "Thailand's National Legislative Assembly Passes Data Protection Law," *Privacy & Information Security Law Blog*, last modified March 15, 2019, accessed June 5, 2019, https://www.huntonprivacyblog.com/2019/03/15/thailands-national-legislative-assembly-passes-data-protection-law/.

economy"[1089] issued a new Data Protection Regulation which draws many concepts from the GDPR.[1090]

Notably, some steps towards the EU model have also been taken in the US which, as seen above, has often been mentioned as the most evident example of how data protection can be tackled with a completely different approach compared to the EU. More specifically, in 2018, the State of California adopted the California Consumer Privacy Act (CCPA), which regulates the processing of personal data on a *comprehensive* (as opposite to the traditional sectorial) manner. The CCPA, which will become effective in 2020, overlaps on several points with the GDPR in its attempt to give consumers more control over their data: it recognizes the right to erasure; the right to be informed by organizations about the collection and the processing of personal data; the right of access; and the right to data portability. At the same time, the CCPA differs from the GDPR is some substantial ways. For example, the CCPA does not include the principle under which data can only be processed on the basis of a legal ground, which is instead one of the core principles upon which the GDPR is grounded (Article 6 GDPR). Moreover, most of the obligations prescribed by the CCPA only apply to *for-profit* entities that meet specific thresholds (e.g., annual gross revenue in excess of $25 million) while the GDPR applies to any "controller" irrespective of whether its activities are for-profit or not. As a further difference, the GDPR protects any "data subject" while the CCPA affords rights to individuals who are *resident* in California.[1091]

[1089] Preamble, Nigeria Data Protection Regulation (2019). The text of the Regulation is available at: https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf.

[1090] "Nigeria Issues New Data Protection Regulation," *Privacy & Information Security Law Blog*, last modified April 5, 2019, accessed June 5, 2019, https://www.huntonprivacyblog.com/2019/04/05/nigeria-issues-new-data-protection-regulation/; Michael Ango and Samuel Ibrahim, "Data Protection Regulation 2019: An Emerging Frontier in Data Management in Nigeria," *Andersen Tax Digest*, April 23, 2019, accessed June 5, 2019, https://andersentax.ng/data-protection-regulation-2019-an-emerging-frontier-in-data-management-in-nigeria/. For an overview of other countries which in 2018 have amended or have started the process of amending their privacy laws to align them with the GDPR, see "Data Privacy Law: The Top Global Developments in 2018 and What 2019 May Bring," *DLA Piper*, last modified February 25, 2019, accessed June 4, 2019, https://www.dlapiper.com/en/belgium/insights/publications/2019/02/data-privacy-law-2018-2019/.

[1091] For an overview of the similarities and the differences between the GDPR and the CCPA, see Data Guidance and Future of Privacy Forum, *Comparing Privacy Laws: GDPR v. CCPA*, 2018, accessed May 26, 2019, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf; Lydia de la Torre, "GDPR Matchup: The California Consumer Privacy Act 2018," *Iapp*, July 31, 2018, accessed May 26, 2019, https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/.

A discussion is also ongoing at the federal level about the opportunity to replace the sectorial approach that has traditionally characterized the US legislative framework in the data protection field with a more comprehensive approach. Indeed, although the US is still lacking a federal privacy law, some calls in this respect have been advanced by several parties. For example, in January 2019, the US Government Accountability Office released a report where it suggested that "this is an appropriate time for Congress to consider comprehensive Internet privacy legislation".[1092] Indeed, "[c]omprehensive legislation addressing Internet privacy that establishes specific standards ... could help enhance the federal government's ability to protect consumer privacy, provide more certainty in the marketplace as companies innovate and develop new products using consumer data, and provide better assurance to consumers that their privacy will be protected".[1093]

Moreover, in February 2019, the US Chamber of Commerce proposed a model privacy legislation calling for the Congress to replace the current "confusing patchwork of state laws" with a federal consumer privacy law. The model is based on several principles established in the new California's privacy act as well as on data security elements enshrined in the GDPR, such as breach notification requirements. Transparency about how personal data are processed by businesses; consumer control by means of opt-out and data deletion provisions; support for innovation by means of regulatory certainty; and effective enforcement by the Federal Trade Commission are some of the principles that, on the basis of this model, should be endorsed by the Congress in drafting a federal privacy legislation.[1094] Several Senators have also introduced proposals on what a new federal bill setting out data protection standards should look like. Among others, it is worth mentioning the Data

[1092] United States Government Accountability Office, *Report to the Chairman, Committee on Energy and Commerce, House of Representatives. INTERNET PRIVACY - Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, 2019, 38, accessed May 24, 2019, https://assets.documentcloud.org/documents/5736212/GAO-privacy-report.pdf.

[1093] Ibid., 39.

[1094] "U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Federal Privacy Law," *U.S. Chamber of Commerce*, last modified February 13, 2019, accessed May 25, 2019, https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law. The full text of the model privacy legislation is available at: https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf.

Care Act introduced in December 2018 by Senator Brian Schatz and co-sponsored by 14 Senators,[1095] and the proposal released by Senator Ron Wyden which could even lead the imprisonment of executives who fail to follow the new rules.[1096] On November 26, 2019, a new federal privacy bill, called Consumer Online Privacy Rights Act, was introduced by US Senator Maria Cantwell to "provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement".[1097]

Similar calls have also come from the industry. For example, at the 2018 International Conference of Data Protection and Privacy Commissioners, Tim Cook, Chief Executive Officer of Apple Inc., stressed that the US should follow the example set by the EU by adopting a comprehensive federal privacy law. In his view, such privacy law should be rooted in four essential fundamental rights: data minimization; the right to knowledge; the right to access; and the right to security.[1098] Along the same lines, in December 2018, Business Roundtable, an association of chief executive officers of the American largest companies, released a framework for a federal consumer privacy law, urging the Congress to pass a national privacy law in order to expand consumers' rights with regards to their personal data.[1099]

In this framework of *de facto* approximation of the laws of different countries, the EU institutions seem to be willing to foster the role of the European Union as a driver for the development

---

[1095] The text of the proposed Data Care Act is available at: https://www.schatz.senate.gov/imo/media/doc/Data%20Care%20Act%20of%202018.pdf.

[1096] Rob Pegoraro, "Why 2019 Might Finally Bring a National Privacy Law for the US," *Yahoo! Finance*, last modified December 31, 2018, accessed May 25, 2019, https://finance.yahoo.com/news/why-2019-might-finally-bring-144821100.html; Rachel E. Ehlers, "The Data Care Act of 2018," *The National Law Review*, December 27, 2018, accessed May 25, 2019, https://www.natlawreview.com/article/data-care-act-2018; Colin Lecher, "Democratic Senators Have Introduced a Big New Data Privacy Plan," *The Verge*, last modified December 12, 2018, accessed May 25, 2019, https://www.theverge.com/2018/12/12/18138131/democratic-data-care-act-senate-law; Colin Lecher, "Sen. Ron Wyden Proposes Bill That Could Jail Executives Who Mishandle Consumer Data," *The Verge*, last modified November 1, 2018, accessed May 25, 2019, https://www.theverge.com/2018/11/1/18052254/ron-wyden-privacy-bill-draft-consumer-tracking.

[1097] The text of the proposed Consumer Online Privacy Rights Act is available at: https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf.

[1098] Tim Cook, "Remarks before the International Conference of Data Protection & Privacy Commissioners" (Brussels, Belgium, October 24, 2018), accessed May 24, 2019, https://www.privacyconference2018.org/system/files/2018-10/Tim%20Cook%20speech%20-%20ICDPPC2018.pdf.

[1099] "Business Roundtable Releases Framework for National Consumer Privacy Law," *Business Roundtable*, last modified December 6, 2018, accessed May 25, 2019, https://www.businessroundtable.org/business-roundtable-releases-framework-for-national-consumer-privacy-law; Business Roundtable, *Framework for Consumer Privacy Legislation*, 2018, accessed May 25, 2019, https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf.

of international standards. For example, in the 2010 Stockholm Programme ("An Open and Secure Europe Serving and Protecting Citizens"), the Council of the European Union stressed the role that the Union should play as "a driving force behind the development and promotion of international standards for personal data protection, based on relevant Union instruments on data protection and the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and in the conclusion of appropriate bilateral or multilateral instruments".[1100] The same concept was expressed the same year by the European Commission:

> Data processing is globalised and calls for the development of universal principles for the protection of individuals with regard to the processing of personal data. The *EU legal framework for data protection* has often served as a *benchmark for third countries* when regulating data protection. Its effect and impact, within and outside the Union, have been of the utmost importance. The European Union must therefore remain a *driving force behind the development and promotion of international legal and technical standards* for the protection of personal data, based on relevant *EU* and *other European instruments* on data protection. This is particularly important in the framework of the EU's enlargement policy.[1101]

In other words, the European Commission stressed the importance of "[p]romoting universal principles", which, notably, it identified with the principles enshrined in the EU data protection framework and in other European instruments. In the same vein, in its 2015-2019 Action Plan, the EDPS stressed that Europe "needs to be at the forefront of *shaping a global standard for privacy and data protection*, a standard centred on the rights and the dignity of the individual. The EU has a window of opportunity to adopt the future-oriented standards that we need, standards that inspire others at global level".[1102] In other words, according to the EDPS, the EU has a "unique chance to *shape* a *global, digital standard* for the respect of *privacy* and the *protection of personal information*".[1103]

[1100] Council of the European Union, *The Stockholm Programme – An Open and Secure Europe Serving and Protecting the Citizens* (Brussels, 2009), paragraph 2.5, accessed June 10, 2016, https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/the_stockholm_programme_-_an_open_and_secure_europe_en_1.pdf.

[1101] European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union*, COM(2010) 609 final. (Brussels, 2010), paragraph 2.4.1 (italics mine), accessed May 29, 2019, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.

[1102] European Data Protection Supervisor, *Leading by Example: The EDPS Strategy 2015-2019*, 2015, 7 (italics mine), accessed June 1, 2019, https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf.

[1103] Ibid., 16 (italics mine).

Moreover, as noted by the Special Rapporteur on the Right to Privacy, the influence that the GDPR exerts across the globe emerges not only from the adoption by non-EU countries of GDPR-like data protection laws but also from the fact that several companies operating globally have started, of their own volition, to adopt GDPR-compliant policies across their global operations. Companies operating globally has hence started to extend the standards of protection established under the GDPR to their non-EU based customers irrespective of a legal obligation to do so: "[t]his 'GDPR-creep' may be just as significant as legislative adoption".[1104] The tendency of companies operating globally to align their policies to the GDPR was also acknowledged by the European Commission in its 2017 communication to the European Parliament and the Council: "companies recognise that strong privacy protections give them a competitive advantage as confidence in their services increases. Many, especially those with global reach, are aligning their privacy policies with the GDPR, both because they want to do business in the EU, and because they see it as a model to follow".[1105]

The EU framework has hence shown its power to influence not only the legislative process of third countries but also the behaviour of commercial actors operating across various countries.[1106] For example, in 2018, Facebook announced its plan to implement the GDPR across its global network of users. The (stated) aim is to put Facebook users in more control over their data by developing new privacy tools that will be made available everywhere, and not just to users in the Union.[1107] Google has even enshrined this commitment in its DP Agreement. Indeed, the clause on the "application of terms" provides that "[e]xcept to the extent these Terms state otherwise, these Terms will apply irrespective of whether European Data Protection Law or Non-European Data Protection Law applies

[1104] United Nations General Assembly, *Report of the Special Rapporteur on the Right to Privacy*, paragraph 99.

[1105] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 2.

[1106] Kuner, *The Internet and the Global Reach of EU Law*, 25.

[1107] Gerard Stegmaier and Ariana Goodell, "Facebook Announces Plan to Implement GDPR Globally," *ReedSmith - Technology Law Dispatch*, last modified April 9, 2018, accessed May 28, 2019, https://www.technologylawdispatch.com/2018/04/privacy-data-protection/facebook-announces-plan-to-implement-gdpr-globally/; Sarah Jeong, "Zuckerberg Says Facebook Will Extend European Data Protections Worldwide — Kind Of," *The Verge*, last modified April 11, 2018, accessed May 28, 2019, https://www.theverge.com/2018/4/11/17224492/zuckerberg-facebook-congress-gdpr-data-protection.

to the processing of Customer Personal Data".[1108] Organizations operating globally are hence increasingly incorporating the GDPR standards into their global corporate privacy policies and procedures. Long story short, "whether by law or through practice", the EU has become an international data protection standard.[1109]

All these elements prove that despite the diversity in cultural and historical traditions, and the pressure of several and often diverging political and economic considerations, a certain degree of international harmonization *can* be achieved and *has been* achieved[1110] and this gradual convergence may reduce the need for restricting data flow. Indeed, as shown above, the GDPR and the DPD before it – together with Convention 108 – has offered to other jurisdictions a template of provisions to emulate and implement, thus acting as an "instrument of harmonization".[1111]

6.2.5. Long-term and Short-term Effects of National and International Developments in the Data Protection Field

A line should be drawn between long-term effects of recent developments in the data protection field, namely the desirable, yet still unlikely, development of global and legally binding data protection standards, and short-term effects of such developments. Indeed, it can be argued that, although a global data protection agreement (as the most desirable long-term solution) is still far from been reached, the globalisation of Convention 108 and the adoption of GDPR-like data protection legislation by non-EU countries may have some *immediate* (i.e., short-term) positive effects. As a first short-term effect, it is worth noting that the *de facto* approximation of the laws of different countries may reduce, at least to some extent, the multiplication of operational efforts that often

[1108] Section 4.3, Google, Data Processing and Security Terms (Customers), accessed December 17, 2019, https://cloud.google.com/terms/data-processing-terms.

[1109] Clare Sullivan, "EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era," *Computer Law & Security Review* 35, no. 4 (2019): 397.

[1110] Prins, "Should ICT Regulation Be Undertaken at an International Level?," 173.

[1111] Bennett, "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?," 243–244.

burden and puzzle companies that operate at a global level and that are hence confronted with a bewildering number of different (although not always conflicting)[1112] legal requirements.

Indeed, even in the absence of a global data protection treaty, this indirect convergence may be extremely beneficial for companies that often need to navigate between divergent national data protection requirements they are unaware of or they know nothing about. Kuner (2010), for example, noted that even though the possibility of achieving harmonization of data protection law is unlikely, reaching a certain degree of harmonization of some key concepts of data protection law, like what constitutes "personal data", seems to be feasible and it "would go a long way to ensuring that EU data protection law applies only where a real and important data protection interest of the individual and of the State is involved".[1113] Interestingly, the development of common definitions of the key data protection terms is one of the actions that the ICDPPC has included in its strategic plan 2019-2021 as one of the steps to achieve a "global regulatory environment with clear and consistently high standards of data protection for all".[1114] A minimization of the differences between national legislations would hence relieve companies operating globally of the compliance challenges that affect their business and which often lead to *non*-compliance. Many organizations may in fact not be able, or willing, to tailor their services to meet the specific requirements of every single jurisdiction in which they operate.[1115]

At the same time, however, it should be stressed that the implementation of GDPR-related measures would not automatically exempt companies from adopting other jurisdiction-specific measures. In other words, although the GDPR is one of the strictest and most comprehensive data protection frameworks in the world, complying with GDPR would not make companies compliant

[1112] "From a practical perspective, it is worth noting that these stricter requirements [set by the laws of non-EU countries] do not conflict with the GDPR. Companies can – and must – comply with the stricter requirement. When counsel clients on GDPR compliance, I point out these additional requirements and help companies take care of all requirements at the same time". Daniel Solove, "Beyond GDPR: The Challenge of Global Privacy Compliance - An Interview with Lothar Determann," *PRIVACY + SECURITY BLOG*, November 13, 2017, accessed May 27, 2019, https://teachprivacy.com/challenge-of-global-privacy-compliance/.

[1113] Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)," 242–243.

[1114] 41st International Conference of Data Protection and Privacy Commissioners, *Resolution on the Conference's Strategic Direction (2019-21)*, 7.

[1115] Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 102.

with all other jurisdictions. Indeed, although a certain degree of convergence has been achieved thanks to the influence exerted by the European standards around the globe, many other countries provide for more specific, and sometimes stricter requirements which companies need to address separately from the GDPR requirements. In this context, companies will need to "prioritize based on their resources, locations, business focus, customer expectations and risk profile".[1116]

Moreover, as a second short-term effect, both the *de facto* approximation of the laws and the ratification of Convention 108 may have some immediate positive effects in boosting international data flow. Indeed, States that have adopted GDPR-like data protection legislation are more likely to be found adequate by the European Commission. This has been confirmed in 2017 by the European Commission:

> In recent years *more and more countries around the world have adopted new legislation in the area of data protection and privacy or are in the process of doing so*. In 2015, the number of countries that had enacted data privacy laws stood at 109, a significant increase from 76 in mid-2011. Moreover, around 35 countries are currently drafting data protection laws. These new or modernised laws tend to be based on *a core set of common principles*, including inter alia the recognition of data protection as a fundamental right, the adoption of overarching legislation in this field, the existence of enforceable individual privacy rights, and the setting up of an independent supervisory authority. This offers *new opportunities, notably through adequacy findings, to further facilitate data flows while guaranteeing the continued high level of protection of personal data*.[1117]

The European Commission has hence recognized that the adoption by an increasing number of countries of data protection rules that are in line with the EU data protection framework may ease the adoption of adequacy findings and, consequently, ease international data flow without compromising the high standards for data protection set out within the EU.

Moreover, it should be recalled that the ratification of Convention 108 is one of the elements that the Commission values when assessing the level of protection guaranteed by a third country. Recital 105 GDPR, indeed, provides that in assessing the level of protection afforded by a third country, the Commission should also take account of the "obligations arising from the third country's

[1116] Solove, "Beyond GDPR: The Challenge of Global Privacy Compliance - An Interview with Lothar Determann."

[1117] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 7 (italics mine).

or international organisation's participation in multilateral or regional systems ...". In particular, "the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account".[1118] The ratification of Convention 108 may hence facilitate, although not guarantee (since, as seen in 6.2.2.3., some principles included in the GDPR are not incorporated in the Convention), the adoption of adequacy decisions by the European Commission.[1119]

6.3. Solution 2: Solving Data Transfer Issues by Means of Rules on Applicable Law

6.3.1. Scope of the Section

As seen above (5.9.1.), it has been argued that the extra-territorial scope of the GDPR may make, at least to some extent, data transfer provisions superfluous when the processing of the transferred data falls entirely under the scope of the GDPR (this is what I have called "jurisdictional approach"). As Kuner (2010) posits, "it seems redundant and inefficient to use two sets of legal provisions (namely those concerning applicable law and transborder data flows) to fulfil the same purpose, namely protecting personal data processed outside the geographic boundaries of the EU".[1120] Given this seemingly unnecessary overlap between the rules on applicable law set out under Article 3 GDPR and data transfer provisions, some have argued that the transfer of data to non-EEA entities that directly fall under the territorial scope of the GDPR should not be restricted since the purpose of data transfer provisions, i.e., avoiding circumvention of the EU data protection legislation, is already achieved by the rules on applicable law. This "solution" seems particularly appealing considering that by abandoning data transfer provisions, all the inefficiencies and impracticalities of these

[1118] Recital 105, GDPR.

[1119] Greenleaf, *Convention 108+ and the Data Protection Framework of the EU*, 4–5. At the same time, it should be noted that some countries may be considered adequate by the European Commission but not eligible for acceding to Convention 108. Indeed, the requirements against which adequacy is assessed may be satisfied by provisions which only apply to personal data transferred from the European Union, such as in the case of the Privacy Shield, while "Convention 108+ accession requires provisions which apply to all personal data within a country's jurisdiction (not only that coming from 108+ Parties)". Ibid., 4.

[1120] Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, 43.

provisions in enabling data transfer would also be abandoned without undermining their ultimate aim. The spirit of data transfer provisions (i.e., effective protection of transferred data) would so be preserved without, however, imposing on data exporters/importers compliance with often merely formalistic mechanisms. Simply put, at first sight, substance would prevail over bureaucracy and formalisms.[1121]

The above considerations can be summarized in the following statement: *there is no added value in implementing data transfer provisions when the data importer is directly subject to the GDPR*. In order to understand to what extent this statement is correct, it should be analysed against the following scenarios:

1. transfer from an EEA controller to a non-EEA processor subject to GDPR;
2. transfer from an EEA controller to a non-EEA processor *not* subject to GDPR;
3. transfer from an EEA controller to a non-EEA controller subject to GDPR;
4. transfer from an EEA controller to a non-EEA controller *not* subject to GDPR.

These scenarios will be analysed in the following pages.

6.3.2. Transfer of Data from EEA Controllers to non-EEA Processors

Let's first consider scenarios 1 and 2 which, as seen above, entail the transfer of data from an EEA controller to a non-EEA processor. It should first be recalled that under Article 28(3) GDPR, the "[p]rocessing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller".[1122] Regardless of the presence of an international data transfer, the GDPR hence requires that the relationship between controllers and processors is governed by a DP Agreement that details the subject-matter, the nature

[1121] As noted by Kuner, "[t]he regulation of international data transfers relies heavily on bureaucratic, formalistic measures, including the signature of contractual clauses, consent clauses in online forms, lengthy processes for the approval of BCRs by DPAs, filings of forms with DPAs where companies provide information about their data processing and data transfer practices, and other similar mechanisms. The procedure for having third countries declared 'adequate' by the European Commission is also a triumph of bureaucracy and formalism over substance, and has been criticized as inefficient, untransparent, and subject to political influence". "Reality and Illusion in EU Data Transfer Regulation Post Schrems," 911.

[1122] Article 28(3) GDPR.

and the purpose of the processing, its duration, the type of personal data and categories of data subjects involved, the controller's and processor's obligations and respective rights.[1123] It is worth noting that the contractual requirements that shall be included in DP Agreements are now set out under Article 28 GDPR in a much more detailed fashion compared to Article 17 DPD.[1124] Indeed, while Article 28 GDPR sets out a whole list of the requirements that should be included in these agreements, Article 17 DPD solely provided that DP Agreements must stipulate that (a) "the processor shall act only on instructions from the controller" and that (b) the obligation to implement appropriate technical and organizational measures to protect personal data shall be incumbent on processors as on controllers.[1125]

In the light of this, instead of investigating the added value of implementing data transfer provisions when the data importer is directly subject to the GDPR, when data are transferred to a non-EEA data processor, another question is worthy of being explored: *when data are transferred to non-EEA data processors, what is the added value of implementing data transfer provisions when a DP Agreement is already in place?* After all, even if non-EEA processors are not directly subject to the GDPR, they are contractually bound to follow the instructions of the EEA controller which, in turn, is directly subject to the GDPR and will hence remain liable to data subjects and subject to DPA's enforcement powers.[1126] In other words, it could be argued that, as a normative matter, the implementation of SCCs (or other transfer mechanisms) is superfluous in ensuring continued compliance with the GDPR when data are transferred to a non-EEA processor: if the EEA controller

[1123] Article 28(3) GDPR.

[1124] For an analysis of the requirements that should be included in DP Agreements see, among others, David White and Tom Morrison, "Mind the GDPR: Processors & Data Processing Agreements," *New Law Journal* 168, no. 7788 (2018): 12–13; Jenna Lindqvist, "New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?," *International Journal of Law and Information Technology* 26, no. 1 (2018): 45–63; John Clarke, "Data-Processing Agreements from 30,000 Feet," *Iapp*, May 22, 2018, accessed March 7, 2019, https://iapp.org/news/a/data-processing-agreements-from-30000-feet/.

[1125] Article 17(3) DPD.

[1126] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 53 and 184. Hon pushed this reasoning even further in stating that, in principle, controllers remain liable under the EU data protection legislation even if they have not entered into any DP Agreement with their EEA or non-EEA processors. However, she also acknowledged that "implementing such contracts obviously facilitates compliance" with their obligations under the GDPR. Ibid., 64.

is *legally* bound to process data in compliance with the GDPR and if the processor, whether within or outside the EEA borders, is *contractually* bound to follow the instructions of the EEA controller by virtue of the DP Agreement, such DP Agreement alone seems to be well-suited and sufficient to achieve the anti-circumvention objective. As Hon (2017) posits, if legal measures, such as DP Agreements, "can adequately restrict processors from using, disclosing or modifying personal data without the controller's authority, then logically why should SCCs or the like be required in addition, just because personal data are to be processed in non-EEA locations?".[1127]

In order to answer the question whether the implementation of SCCs adds any value in protecting data when a DP Agreement is already in place, the table below will compare the provisions under 2010 SCCs (i.e., controller-processor SCCs) and the provisions that under Article 28 GDPR shall be included in DP Agreements:

	Art.28 DP Agreement	**2010 SCCs**	**COMMENTS**
1	Art.28(3) **Description of the processing** The parties must specify: • the subject-matter and duration of the processing; • the nature and purpose of the processing; • the type of personal data and categories of data subjects; • the obligations and rights of the controller.	Clause 2 Appendix 1 **Details of the transfer** The parties must specify: • the activities conducted by the data exporter and by the data importer respectively that are relevant to the transfer; • the processing operations to which the transferred data will be subject • the type of personal data and categories of data subjects concerned by the transfer.	Clause 2 and Appendix 1 of the SCCs do not include the obligation to specify the duration of the processing.
2	Art.28(3)(a) **Documented instructions** The processor shall process the personal data only on	Clause 5 **Obligation of the data importer** The data importer agrees and warrants:	Under Article 28, the data processor is not required to promptly inform the controller of its inability to comply with the controller's instructions for whatever

[1127] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 223–224. Similar arguments have been put forward by several authors and lobbies when the Commission decision on SCCs for EEA controller – non-EEA processor transfers was first issued. On this point see, Yves Poullet, Sophie Louveaux, and Maria Veronia Perez Asinari, "Data Protection and Privacy in Global Networks: A European Approach," *The EDI Law Review* 8 (2001): 174.

	documented instructions from the controller.	• to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract (clause 5(a)); • that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract (clause 5(b)).	reasons. Moreover, Article 28 does not include the data importer's obligation to warrant that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the SCCs.
3	Art.28(3)(a) **International data transfers** The processor shall not perform transfers of personal data to a third country or to an international organisation without the prior permission of the controller.		SCCs do not specifically refer to the obligation to obtain the prior permission of the controller before engaging in onward transfers. However, this obligation can be inferred from the general obligation to follow the instructions of the controller/data exporter under Clause 5(a).
4	Art.28(3)(b) **Confidentiality** The processor shall ensure that persons authorised to process the personal data have		SCCs do not include any provision under which the data importer commits to confidentiality when processing the transferred data. The only representation

	committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.		by the data importer concerning confidentiality can be found in clause 12(1) under which the data importer warrants that it will guarantee the confidentiality of the transferred data *after* the termination of the provision of the personal data-processing services.
5	Art.28(3)(c) **Security of processing** The processor shall take the security measures specified under Article 32 GDPR.	Clause 5(c) Appendix 2 **Security of processing** The data importer agrees and warrants that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred.	This requirement is included in both Article 28 GDPR and SCCs.
6	Art.28(2) Art.28(3)(d) **Subcontracting authorization** The processor shall not engage another processor without prior specific or general written authorisation of the controller.	Clause 5(h)-5(j) Clause 11(1) **Subcontracting authorization** The data importer agrees and warrants that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent and to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.	This requirement is included in both Article 28 GDPR and SCCs.
7	Art.28(4) Art.28(3)(d) **Obligations in the event of subcontracting** Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as	Clause 11(1) **Obligations in the event of subcontracting** Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed	This requirement is included in both Article 28 GDPR and SCCs.

	referred to in Article 28(3) shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law.	on the data importer under the Clauses.	
8	Art.28(3)(d) Art.28(4) **Liabilities in the event of subcontracting** Where the sub-processor engaged by the processor under Article 28(4) fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	Clause 11(1) **Liabilities in the event of subcontracting** Where the sub-processor fails to fulfil its data protection obligations under the written agreement with the data importer, the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.	This requirement is included in both Article 28 GDPR and SCCs.
9	Art.28(3)(e) **Assisting controllers in responding to data subjects' requests** The processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.	Clause 5(d)(iii) **Notification of data subjects' requests** The data importer agrees and warrants that it will promptly notify the data exporter about any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so. Clause 5(e) **Duty to cooperate with the data exporter** The data importer agrees and warrants to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer.	Even if SCCs do not specifically include the data importer's obligation to cooperate with the data exporter in responding to data subjects' requests, such obligation can be inferred from Clauses 5(d)(iii) and 5(e).
10	Art.28(3)(f) **Assisting controllers in compliance with security requirements** The processor shall assist the controller in ensuring		No specific provision is included in SCCs that prescribe that the data importer shall assist the controller in ensuring compliance with its own security obligations.

	compliance with the obligations pursuant to Articles 32 (security measures)		
11	Art.28(3)(f) **Assisting controllers in responding to data breach** The processor shall cooperate with the controller in the event of data breach (Article 33-34 GDPR)	Clause 5(d)(ii) **Notification in the event of accidental or unauthorised access** The data importer agrees and warrants that it will promptly notify the data exporter about any accidental or unauthorised access.	Clause 5(d)(ii) only refers to "accidental or unauthorised access" which is a subset of what constitutes a "data breach" under the GDPR.[1128] In addition, no reference is made to the timing requirement for notifying the competent DPA of the data breach occurred.
12	Art.28(3)(f) **Assisting controllers in conducting DPIA** The processor shall assist the controller in conducting data protection impact assessments (Article 35-36 GDPR).		SCCs do not stipulate that the non-EEA processor shall assist the controller in conducting DPIAs.
13	Art.28(3)(g) **Obligation to delete or return the data** The processor shall delete or return all the personal data to the controller after the end of the provision of services relating to processing.	Clause 12(1) **Obligation to destroy or return the data** The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so.	This requirement is included in both Article 28 GDPR and SCCs.
14	Art.28(3)(h) **Audit rights** The processor shall allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.	Clause 5(f) **Audit rights** The data importer agrees and warrants that at the request of the data exporter it will submit its data-processing facilities for audit of the processing activities covered by the Clauses. Such audit shall be	This requirement is included in both Article 28 GDPR and SCCs. Unlike Art.28(3)(h), Clause 12(2) also explicitly provides that an audit may be conducted to demonstrate compliance with the obligations under Article 12(1) SCCs (i.e., return or destroy the transferred

[1128] Article 4(12) GDPR defines "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

		carried out by the data exporter or an inspection body selected by the data exporter, where applicable, in agreement with the supervisory authority. Clause 12(2) **Audit rights** The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the implementation of the measures required by clause 12(1) after termination of personal data-processing services.	personal data after the termination of the personal data-processing services).
15		Clause 5(d)(i) **Requests from law enforcement authorities** The data importer agrees and warrants that it will promptly notify the data exporter about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited.	No similar obligation is included under Article 28 GDPR.
16		Clause 3 **Third-party beneficiary clause**[1129] The data subject can enforce several clauses against the data exporter. The data subject can also enforce several clauses against the data importer in cases where the data exporter has factually disappeared or has ceased to exist in law. The data subject can also enforce some clauses against the sub-processor for	No third-party beneficiary clause is included under Article 28 GDPR.

[1129] See also clause 5(g) 2010 SCCs, under which the data importer agrees and warrants "to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing...".

		its own processing operations in cases where both the data exporter and the data importer have factually disappeared or have ceased to exist in law or have become insolvent.	
17		Clause 4 **Obligations of the data exporter** The data exporter agrees and warrants: • that the processing will continue to be carried out in accordance with EU data protection law (clause 4(a)); • that it has given and it will continue to give instructions to the data importer (clause 4(b)); • that the data importer will provide sufficient guarantees in respect of technical and organisational security measures (clause 4(c)); • that the security measures are appropriate to protect data against any unlawful forms of processing (clause 4(d)); • that it will ensure compliance with security measures (clause 4(e)); • that the data subjects have been informed or will be informed before, or as soon as possible after, the transfer of special categories of data to non-adequate countries (clause 4(f)); • that it will forward any notification received from the data importer or any sub-processor pursuant to	Even if some of the provisions under clause 4 are not listed under Article 28, most of the data exporter's obligations listed under this clause can be inferred from other GDPR provisions: • clause 4(a) SCCs → This obligation is guaranteed by the general applicability of the GDPR to the EEA data exporter/controller; • clause 4(b) SCCs→ Art.28(3) GDPR; • clause 4(c) SCCs→ Art.28(1) GDPR; • clause 4(d) and 4(e) SCCs → Art.24 and Art.32 GDPR; • clause 4(f) SCCs → Art.13(1)(f) and Art.14(1)(f) GDPR;[1130] • clause 4(f) SCCs → Art.13(1)(f) and Art.14(1)(f) GDPR; • clause 4(h) SCCs → Art.13(1)(f), Art.14(1)(f) and Art.15 GDPR; • clause 4(i) SCCs→ Art.28(2), Art.28(3)(d) and Art.28(4). On the other hand, the requirement under clause 4(g) has no explicit counterpart in the GDPR**.**

[1130] It should be noted that under clause 4(f), data subjects shall be informed of the transfer only when special categories of data are concerned, while the requirements under Art.13(1)(f) and Art.14(1)(f) apply to transfers of any personal data.

		Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension (clause 4(g)); • that it will make available to the data subjects upon request a copy of the Clauses, as well as a copy of any contract for sub-processing services (clause 4(h)); • that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer (clause 4(i)).	
18		Clause 6 **Liability**[1131] • The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 (Third party beneficiary clause) or in Clause 11 (sub-processing) by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered (clause 6(1)); • the data importer agrees that the data subject may issue a claim against the	No liability clause is included under Article 28 GDPR. However, the general rule under article 82 GDPR apply ("Right to compensation and liability")

[1131] In connection with clauses 3 and 6, see also clause 7: "1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject: (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority; (b) to refer the dispute to the courts in the Member State in which the data exporter is established. 2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law".

		data importer as if it were the data exporter, if the data subject is not able to bring a claim for compensation against the data exporter because the data exporter has factually disappeared or ceased to exist in law or has become insolvent (clause 6(b)); • the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations as if it were the data exporter or the data importer, if a data subject is not able to bring a claim against the data exporter or the data importer because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent.	
19		Clause 8 **Cooperation with supervisory authorities** • The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law (clause 8(2)); • the data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor. In such a case the data exporter shall be entitled to suspend the	No obligation to cooperate with supervisory authorities is included under Article 28 GDPR. However, Article 31 GDPR applies. Article 31 requires the controller and the processor to "cooperate, on request, with the supervisory authority in the performance of its tasks".

		transfer of data and/or terminate the contract pursuant to Article 5(b) (clause 8(3)).	
20		Clause 9 **Governing Law** The Clauses shall be governed by the law of the Member State in which the data exporter is established.	No similar provision is included under Article 28 GDPR.

Table 11 – Comparison Article 28 GDPR – 2010 SCCs[1132]

The analysis conducted above has shown that several clauses under SCCs are also included in DP Agreements so that a duplication of such requirements in two separate contracts (DP Agreements and SCCs) would, indeed, be superfluous. At the same time, however, it is also clear from the table above that some provisions included in SCCs are not incorporated in DP Agreements (and vice versa).[1133] Some of the provisions that are included in SCCs but not in DP Agreements reflect the peculiarities of SCCs, and, in turn, the peculiarities of international data transfers compared to intra-EEA transfers. The most relevant provisions that are included in SCCs but *not* in DP Agreements are the following:

- Clause 3, under which data subjects are entitled to enforce several clauses, firstly, against the data exporter and, in certain circumstances, even against the data importer and the sub-processor (see table 11 requirement number 16).
- Clause 5(a) and Clause 5(b) under which the data importer commits to inform the data exporter of its inability to comply with its instructions and it warrants that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the data exporter's

[1132] In drafting this table, I have used as a reference point the table at slides 38-41 of the following presentation: Bryan Cave Leighton Paisner Data Privacy and Security Team, "Complying with the EU General Data Protection Regulation (GDPR): Cross Border Transfers of Information" (Celesq® AttorneysEd Center, May 1, 2018), accessed April 23, 2019, https://www.bclplaw.com/images/content/1/0/v2/103150/gdpr-5-1-2018.pdf.

[1133] Some of the gaps identified in SCCs that have emerged from the comparison between Article 28 GDPR and SCCs derive from the fact that SCCs have been drafted on the basis of the 1995 Directive which did not include some of the obligations set out the GDPR. For example, the need to carry out a data protection impact assessment for certain types of processing, and the consequent processor's obligation to assist the controller in conducting the DPIA (Art.28(3)(f) GDPR), was first introduced under the GDPR. These gaps are hence likely to be filled when and if the SCCs will be updated.

instructions and that in the event of a change in this legislation it will promptly notify the data exporter (see table 11 requirement number 2).

- Clause 5(d)(i) under which the data importer shall notify the data exporter of any legally binding request for disclosure of the personal data by a law enforcement authority (see table 11 requirement number 15)
- Clause 6, under which data subjects are entitled to receive compensation, firstly, by the data exporter and, in certain circumstances, from the data importer or even from the sub-processor (see table 11 requirement number 18).
- Clause 8, under which the parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor (see table 11 requirement number 19).

The reason why these clauses reflect the peculiarities of international data transfers vis-à-vis intra-EEA transfers derives from the fact that, as noted by the A29WP in several occasions, unlike DP Agreements, SCCs do not only determine how the data protection responsibility should be split between the data controller and the data processor but also "need to supply for the lack of adequate protection in the country of destination".[1134] And in order to do so, contractual solutions should make sure (1) that the parties commit to process the transferred data in compliance with the substantive data protection rules set out in the EU framework (content principles) and (2) that such rules are made effective by means of procedural/enforcement mechanisms.[1135] These are the two elements against which the adequacy of contractual solutions in protecting transferred data should be assessed (5.5.1.1.).

The first requirement (i.e., content principles), responds to the need to avoid the anti-circumvention of the law once data are transferred outside the EEA. Data transfer rules should hence make sure that the EU data protection standards continue to apply to the transferred data. As for this requirement, when data are transferred to non-EEA processors, no specific commitment to follow EU

[1134] Article 29 Data Protection Working Party, *WP47*, 2-3 (paragraph 2).
[1135] Article 29 Data Protection Working Party, *WP12*, 17–21.

data protection rules by the data recipient seems necessary since processors are contractually bound under DP Agreements to act under the controller's instructions. The data exporter will retain control over the data processing and the EU data protection law will continue to apply to the processing conducted by the data importer.[1136] No real circumvention risk can hence be envisaged in controller-processor transfers. This is reflected by the fact that, unlike controller-controller SCCs, under 2010 SCCs, the processor/data importer is not required to warrant that it will process the transferred data in compliance with the EU data protection principles, being this requirement satisfied by the fact that the data recipient commits to follow the controller's instruction.[1137] Clause 11 about sub-processing – and its counterpart under Article 28(2), 28(3)(d) and 28(4) GDPR – then aims to ensure that the level of protection set out in the SCCs, and in the EU legislation more broadly, will be met through all the levels of the contractual chain.[1138]

At the same time, however, as highlighted above, ensuring the applicability of the EU data protection principles is only one of the two requirements that need to be considered when assessing the adequacy of contractual solutions in protecting transferred data from unlawful processing. The applicability of the EU data protection principles (first requirement) need, in fact, to be complemented with mechanisms (second requirement) that ensure the enforceability of such principles by both data subjects (which need to be able to enforce their rights and to obtain appropriate redress when injured), and DPAs (which need to be able to conduct independent investigations of complaints and sanction misbehaviours). After all, "the feasibility and enforceability of any given data protection system are vital elements to assess its adequacy".[1139]

[1136] Ibid., 18 – 19.

[1137] Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 191.

[1138] In commenting on the draft Commission Decision on SCCs for controller-processor transfers then consolidated in Commission decision 2010/87/EU, the A29WP considered that "Clause 11 –Subcontracting— of the Commission's Draft Decision includes the elements necessary to adequately ensure that the whole chain of possible sub processing operations will continue to ensure the level of protection set out by the standard contractual clauses". Article 29 Data Protection Working Party, *WP161*, 5.

[1139] Article 29 Data Protection Working Party, *WP47*, 5 (paragraph 8).

Within the EU, the enforcement of data protection rules is ensured by a system of remedies, liabilities and penalties.[1140] Article 51 GDPR, in fact, prescribes that "[e]ach Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation". The requirements, the tasks and the powers of national data protection authorities, including the power to impose fines, are then detailed under Articles 52, 53, 57 and 58 GDPR. Moreover, the GDPR (and the 1995 Directive before it) lays out several "enforcement rights" that can be exercised by data subjects before national data protection authorities and courts: data subjects are entitled to lodge a complaint with a supervisory authority (Article 77 GDPR) which will then be in charge of handling and investigating such complaints (Article 57(1)(f) GDPR);[1141] they are entitled to exercise their right to an effective judicial remedy "against a legally binding decision of a supervisory authority concerning them" or where the supervisory authority has failed to handle a complaint (Article 78 GDPR); they are entitled to exercise their right to effective judicial remedy against a controller or processor (Article 79 GDPR) from which they can receive compensation when an infringement of the Regulation has caused them material or non-material damage (Article 82 GDPR).[1142] Moreover, even if the monitoring and investigative powers of DPAs are confined within their national borders (Article 55(1) GDPR),[1143] a system of mutual assistance between the supervisory authorities of the EU Member States has been established in order to ensure a consistent and effective application of the Regulation in cross-border cases.[1144]

[1140] Chapter VIII of the GDPR is entitled "remedies, liability and penalties".

[1141] The performance of the tasks of the supervisory authorities shall be free of charge for data subjects (Article 57(3) GDPR) and supervisory authorities shall facilitate the submission of complaints by data subjects "by measures such as a complaint submission form which can also be completed electronically" (Article 57(2) GDPR).

[1142] For an overview of the data subjects' enforcement rights and for a comparison between the GDPR and the 1995 Directive, see P. T. J. Wolters, "The Enforcement by the Data Subject Under the GDPR," *Journal of Internet Law* 22, no. 8 (2019): 22–31.

[1143] Article 55(1): "Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation *on the territory of its own Member State*" (italics mine).

[1144] Articles 51(2), 57(g), 60 ff. GDPR. For an overview of the enforcement of the GDPR in cross-border cases, see European Data Protection Board, *First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities*, 2019, accessed December 26, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

On the contrary, outside the EU, in most cases there is no guarantee that similar procedural means for ensuring compliance with data protection rules are in place thus raising potential enforcement problems for both data subjects and DPAs.[1145] Such enforcement problems are acknowledged by the EU legislators in Recital 116 GDPR which underlines how transfer of data to third countries "may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information". Moreover, DPAs may be restrained in their capacity to pursue and investigate complaints related to the processing activities conducted outside the EU borders: DPAs' efforts to work in a cross-border context may "be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints".[1146]

As also noted by the A29WP in highlighting the main differences between intra-EEA data transfers and international data transfers, the practical result of the process of externalisation of the processing services

> is that large distances and national borders separate the data controller in Europe from the data processor established in a different region of the planet and that while it is true that the enforcement of Supervisory Authorities and national courts can reach the data controller established in the Community, the physical location of the data may be a real problem.[1147]

Indeed, "[t]he physical location of the data in third countries makes the enforcement of the contract or the decisions taken by Supervisory Authorities considerably more difficult".[1148]

Moreover, as a further difference between intra-EEA data transfers and international data transfers, it should also be recalled that, when data are transferred to entities located in third countries,

---

[1145] Article 29 Data Protection Working Party, *WP12*, 5 and 20.

[1146] Recital 116 GDPR. Similar enforcement problems have been highlighted by the OECD: "When personal information moves across borders it may put at increased risk the ability of individuals to exercise privacy rights to protect themselves from the unlawful use or disclosure of that information. At the same time, the authorities charged with enforcing privacy laws may find that they are unable to pursue complaints or conduct investigations relating to the activities of organisations outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints". Organisation for Economic Cooperation and Development, *Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy*, 2007, 4, accessed April 15, 2019, http://www.oecd.org/internet/ieconomy/38770483.pdf.

[1147] Article 29 Data Protection Working Party, *WP47*, 4 (paragraph 4).

[1148] Ibid., 3 (paragraph 2).

the non-EEA data recipient may be required by the law to which it is subject to disclose data to public authorities. While disclosure of data in response to requests from public authorities is permitted within the EU framework as long as such requests are limited to what is necessary in a democratic society, in third countries, "similar limitations on the ability of the state to require the provision of personal data from companies and other organisations operational on their territory may not always be in place"[1149] (5.5.1.1.).

In the light of this, the clauses that have been singled out above have translated the second requirement (i.e., the need for procedural/enforcement mechanisms that ensure compliance with the applicable rules) into contractual obligations. First of all, Clause 3 ("Third-party beneficiary clause") and clause 6 ("Liability") aim to grant data subjects redress and hence full enforceability of their data protection rights. Certainly, even in the absence of these specific contractual obligations the data controller/exporter would remain liable for any damage caused as a result of violations of the data protection legislation, including for violations caused by its processors or sub-processors.[1150] However, these contractual provisions allow the data subject to additionally rely on third-party beneficiary rights and on the exceptional liability of the data importer (and of further sub-processors) in the event that the data exporter has disappeared or has ceased to exist or is in bankruptcy.[1151] Clause 9 on governing law also plays an important role in ensuring a legal remedy to data subjects since the law chosen as the national law applicable to the contract shall enable third-party beneficiaries to enforce the contract.[1152]

[1149] Article 29 Data Protection Working Party, *WP12*, 21.

[1150] Article 82(2) GDPR.

[1151] "In those cases where the Data Exporter does not for whatever reasons instruct the Data Importer properly (legal disappearance and bankruptcy, for example), the data subject should additionally be able to rely on the third party beneficiary rights conferred by the standard contractual clauses to make effective basic data protection rights such as access to his personal data, cancellation, rectification, objection, etc.". Article 29 Data Protection Working Party, *WP47*, 4 (paragraph 4). It should be noted that, in WP47, the A29WP expressed its opinion on the Draft Commission Decision on SCCs (version 31 August 2001) that was then consolidated in Commission decision 2002/16/EC. Such decision was then repealed by Commission Decision 2010/87/EU. However, the considerations expressed by the A29WP with reference to the 2001 Draft Commission Decision on SCCs are still relevant since the commented clauses have remained essentially unvaried in their core provisions.

[1152] Recital 22, Commission decision 2010/87/EU. The contract law of some Member States does not recognize the possibility that a contract stipulated between two parties (in the case in question, the data exporter and the data importer) can confer rights to third parties (in the case in question, data subjects). In those Member States, SCCs are

Clause 8 ("Cooperation with supervisory authorities") also includes "a very important element for the standard contractual clauses to provide sufficient safeguards".[1153] Indeed, such clause has the net effect of contractually expanding the monitoring and investigative powers of DPAs beyond their national borders by conferring to the supervisory authority "the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law".[1154] In other words, EU data protection authorities gain, through the contract, the extra-territoriality powers that they do not have under the law.[1155] At the same time, one could argue that, under certain circumstances, the extraterritoriality of DPAs' power may be sufficiently ensured by the extra-territorial scope of the GDPR. Indeed, if the non-EU data processor is caught under Article 3(2) GDPR,[1156] such processor will be required to comply with the GDPR obligations which are directly applicable to processors and such obligations include the obligation to cooperate with DPAs in the performance of their tasks pursuant to Article 31 GDPR.[1157]

Lastly, the "problem of overriding law" is also dealt with in SCCs, and in particular by clauses 5(a), 5(b) and 5(d)(i). By imposing several information requirements on the non-EEA data importer, these clauses arguably allow the data exporter to retain (some) control over the transferred data. DPAs also retain the power to suspend or to impose a ban on data transfer if this is necessary to protect individuals with regard to the processing of their personal data.[1158] In this regard, Ralf Sauer, the Deputy Head of DG Justice's Unit for International Data Flows and Protection at the European Commission, acknowledged that SCCs can never regulate the law of third countries and hence protect

unavailable. See on this point, Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 191n67.

[1153] Article 29 Data Protection Working Party, *WP47*, 6 (paragraph 8).

[1154] Clause 8(2) SCCs.

[1155] Madge, "GDPR's Global Scope: The Long Story."

[1156] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 20–22.

[1157] Ibid., 12–13.

[1158] See Article 4 Commission decision 2010/87/EU as amended by European Commission, *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*.

data from disproportionate government access. At the same time, he also highlighted that SCCs may play a role in strengthening the possibility of intervention by data protection authorities or in placing additional responsibilities on the data exporter or on the data importer.[1159] Moreover, as seen in 5.5.1.2, according to Advocate General Saugmandsgaard Øe, it is precisely the soundness of the mechanisms for suspending data transfer which makes 2010 SCCs a valid instrument for protecting data across borders.[1160]

The same exercise of comparing and contrasting the provisions under DP Agreements and those included in data transfer mechanisms with the aim of identifying the added value of such mechanisms in protecting data can, of course, be replicated with the other data transfer mechanisms. For example, the need to complement data protection rules (first requirement) with mechanisms that make such rules effective (second requirement) clearly emerge from BCRs. Indeed, BCRs shall not only detail the data protection principles that the BCR members shall follow when conducting their processing activities but also the provisions that guarantee the legal enforceability of such rules both *internally* (meaning that individuals within the corporate group should feel compelled to follow the rules), and *externally* (meaning that the corporate rules should be enforceable by data subjects and data protection authorities).[1161]

Let's consider BCR-Controllers, which cover transfer of data from EEA controllers to non-EEA processors (but also to non-EEA controllers, see on this point 5.5.2.) within the same group. In addition to substantial data protection principles,[1162] BCR-C shall include provisions aimed at delivering a good level of compliance and at guaranteeing enforcement. First and foremost, BCRs shall create third-party beneficiary rights for data subjects, including the right to lodge a complaint before the competent data protection authority or the competent court and, where appropriate, to

[1159] Ralf Sauer, "How the Adequacy Mechanism Works: Progress in the EU's Governance of Cross-Border Data Flows?" (Presented at the Computers, Privacy and Data Protection conference, Brussels, January 30, 2019)..

[1160] Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, *Facebook Ireland and Schrems*, Case C-311/18, paragraph 127.

[1161] Article 29 Data Protection Working Party, *WP74*, 10–13.

[1162] Criterion 6.1.1 for approval of BCRs, Article 29 Data Protection Working Party, *WP256 Rev.01*.

obtain redress and compensation.[1163] It could be argued that, in controller-processor transfers, the added value of this provision is not particularly relevant since, even in the absence of such rules, data subjects could enforce their rights against the EEA data controller, in particular by virtue of Articles 79 and 82 GDPR. BCRs hence allow data subjects to rely on third party beneficiary rights on top of their "enforcement rights" under the GDPR.[1164]

As a complement to these rights, the EU headquarter or another BCR member established in the EEA shall accept responsibility for the (unlawful) actions taken by the other non-EEA members and pay for the damages caused by them.[1165] Again, it could be argued that the fact that the EEA data controller/exporter accepts responsibility for the acts of the non-EEA data processors to which data have been transferred is an expression of the general principle under which controllers are ultimately liable for the overall compliance with the GDPR.[1166] Someone could hence question the added value of this provision. At the same time, however, under the rules, the EEA headquarter or the EEA BCR member with delegated data protection responsibilities does not necessarily coincide with the company/controller that has exported the data to the non-EEA processor responsible for the event giving rise to the damages. In other words, data may be exported by company A (EEA data controller) to company B (non-EEA data importer) and, under the BCRs, company C (EEA data controller that is part of the same group) agrees to take responsibility for any breaches by company B. It is hence clear that BCRs do not merely replicate the rules on liability under the GDPR, but they set out a

[1163] Criterion 1.3 for approval of BCRs, Ibid.

[1164] "The purpose of these rules therefore is limited to guaranteeing that authorisations granted by data protection authorities (which will make possible or lawful a transfer of personal data abroad which would otherwise be unlawful) would not end up depriving data subjects of their right to remedies or compensations from which they would have benefited had the data never left EU territory". Article 29 Data Protection Working Party, *WP74*, 18.

[1165] "The BCRs must contain a duty for the EU headquarters, or the EU BCR member with delegated responsibilities to accept responsibility for and to agree to take the necessary action to remedy the acts of other members outside of the EU bound by the BCRs and to pay compensation for any material or non-material damages resulting from the violation of the BCRs by BCR members. The BCRs must also state that, if a BCR member outside the EU violates the BCRs, the courts or other competent authorities in the EU will have jurisdiction and the data subject will have the rights and remedies against the BCR member that has accepted responsibility and liability as if the violation had been caused by them in the Member State in which they are based instead of the BCR member outside the EU". Criterion 1.4 for approval of BCRs, Article 29 Data Protection Working Party, *WP256 Rev.01*.

[1166] Article 5(2) GDPR; Article 82 GDPR.

framework aimed at facilitating the practical and successful exercise of data subject's rights to obtain redress and compensation.

BCRs shall also include some additional provisions aimed at strengthening the effectiveness of the rules: BCRs shall confirm that the BCR member that has accepted liability for the acts of the other non-EEA members "has sufficient assets to pay compensation for damages resulting from the breach of the BCRs";[1167] it is for the EEA BCR member to prove that the non-EEA BCR member is not liable for the contested violation, and not for the data subject to demonstrate that the third-country company is liable for the violation of the rules;[1168] an internal system of complaint handling should be set up;[1169] appropriate training should be organized to the personnel that is involved in the data processing in order to build awareness;[1170] moreover, and in line with clause 8 of 2010 SCCs, *all* BCR members, and hence including non-EEA members, shall commit to cooperate with the data protection authorities, including acceptance of audits conducted by inspectors of the data protection authorities.[1171] As for the "problem of overriding law", BCRs shall also include a provision under which non-EEA members commit to notify the EEA headquarters or the EEA BCR member with delegated data protection responsibilities and the competent DPA of any legal requirement to which they are subject that may substantially undermine the guarantees provided by the rules.[1172]

The same conclusions can be drawn when data are transferred on the basis of an adequacy decision by virtue of Article 45 GDPR. As seen in 5.4.1., adequacy decisions are taken on the basis of the overall assessment of the level of protection offered by the *legal order* of a third country. Indeed, when assessing the adequacy of the level of protection guaranteed by a third country, the Commission shall take into consideration not only (1) the basic data protection principles applicable to the processing of the transferred data (content principles) but also (2) the means for ensuring their

[1167] Criterion 1.5 for approval of BCRs, Article 29 Data Protection Working Party, *WP256 Rev.01*.
[1168] Criterion 1.6 for approval of BCRs, Ibid.
[1169] Criterion 2.2 for approval of BCRs, Ibid.
[1170] Criterion 2.1 for approval of BCRs, Ibid. As highlighted by the A29WP, a data protection system that is able to deliver a good level of compliance is characterized by a high degree of awareness among data controllers of their obligations (Article 29 Data Protection Working Party, *WP12*, 7.)
[1171] Criterion 3.1 for approval of BCRs, Article 29 Data Protection Working Party, *WP256 Rev.01*.
[1172] Criterion 6.3 for approval of BCRs, Ibid.

effective application since "[e]fficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules".[1173]

This is clearly mirrored in the list of elements that should be taken into account by the Commission when conducting such assessment: not only shall the Commission consider the rule of law, respect for human rights and fundamental freedoms,[1174] data protection rules, professional rules and security measures, the international commitments into which the third country concerned has entered especially in relation to the protection of personal data, but also "effective and enforceable data subject rights and effective administrative and judicial redress" for the data subjects concerned and "the existence and effective functioning of one or more independent supervisory authorities".[1175] Moreover, and consistently with the problem of overriding law identified above with reference to contractual solutions, when assessing the adequacy of the level of protection, a *third* element should be considered by the Commission, i.e., that the system provides for essential guarantees to limit interferences with fundamental rights for law enforcement and national security purposes (5.4.1.).

This is why, and leaving for a moment aside the invalidation risks that it is currently facing (5.4.3.), the Privacy Shield decision sets out not only the Principles applying to the US organizations under the Privacy Shield but also the cooperation duties between US recipients and EU DPAs, the possibilities of redress for individuals, and the Commission's finding that any interference by US public authorities with fundamental rights of the individuals concerned will be limited to what is strictly necessary. Along the same lines, the EU-Japan adequacy decision is not only grounded upon the "adequacy" of the data protection rules that apply once data are transferred to Japanese businesses, but also upon the oversight mechanisms and the avenues for judicial and administrative redress laid out in the Japanese system to ensure the enforcement of the rules. Indeed, if these rules are not

[1173] Article 29 Data Protection Working Party, *Adequacy Referential (Updated) (WP254)*, 3.

[1174] Even if Article 45 generally refers to rule of law, human rights and fundamental freedoms, not all human rights problems are relevant for an adequacy finding but only those which are directly relevant for the protection of transferred personal data. Access to court, for example, is a relevant element: if access to court is not guaranteed, individuals would not enjoy enforceable rights since they would have no possibility of redress in case of violations. Sauer, "How the Adequacy Mechanism Works: Progress in the EU's Governance of Cross-Border Data Flows?".

[1175] Article 45(2) GDPR.

respected, an independent data protection authority (the Personal Information Protection Commission, PPC) will be in charge of investigating the processing activities conducted by the Japanese companies and punish infringements. Moreover, in the event that EU individuals complain about violations of their rights, they can rely on the mediation possibilities offered by the Japanese system; they can complain to the PPC in order to obtain redress, or they can bring an action to a Japanese court in order to obtain compensation or injunctions. Moreover, the European Commission has also assessed the limitations and safeguards offered by the Japanese framework when it comes to government access to the data transferred to the business operators in Japan and concluded that "any interference with the fundamental rights of the individuals whose personal data are transferred from the European Union to Japan by Japanese public authorities for public interest purposes ... will be limited to what is strictly necessary to achieve the legitimate objective in question".[1176]

The need to address not only substantive data protection principles but also the mechanisms that make such principles effective – in particular, redress for data subjects and regulatory oversight – also emerges from the new legal bases for transfer set out under Article 46(2)(e), i.e., codes of conduct, and under Article 46(2)(f), i.e., certification mechanisms. Indeed, both codes of conduct and certification mechanisms shall be coupled with "*binding* and *enforceable* commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards *data subjects' rights*".[1177] Equally, the draft Administrative Arrangement for the transfer of personal data between EEA and non-EEA Financial Supervisory Authorities includes not only the definition of the key data protection concepts and the list of the data protection principles that the Authorities should implement, but also a redress mechanism for data subjects and an oversight mechanism under which an Assessment Group is in charge of carrying out periodic review on the implementation of the safeguards in the Arrangement.[1178]

[1176] Recital 173, EU-Japan adequacy decision.

[1177] Articles 46(2)(e) and 46(2)(f) (italics mine).

[1178] European Data Protection Board, *Opinion 4/2019 on the Draft Administrative Arrangement for the Transfer of Personal Data between European Economic Area ("EEA") Financial Supervisory Authorities and Non-EEA Financial Supervisory Authorities*. The EDPB has also drafted a list of minimum safeguards that shall be included in international

In the light of the analysis conducted above, it can be argued that, in controller-processor transfers, investigating whether the implementation of data transfer provisions has any added value in protecting data when the data importer is directly subject to the GDPR bears little relevance. Non-EEA data processors are, in fact, always *in*-directly subject to the obligations set out under the Regulation by virtue of the contractual arrangements under Article 28 which will always need to be implemented regardless of the processor's location.

Still, it can be concluded from this analysis that such an *in*-direct applicability of the EU data protection standards to the non-EEA data recipient is unfit to entirely satisfy the requirements for assessing the adequacy of a system (under Article 45 GDPR) or of other safeguards (under Article 46 GDPR) in protecting transferred data. Indeed, while DP Agreements seem to successfully fulfil the first requirement (i.e., content principles) by contractually expanding the applicability of EU data protection principles outside the EEA, they seem unsuited, or at least not entirely suited, to deal with the specific enforcement and procedural challenges (as well with the challenges posed by the problem of overriding laws) that arise when data are transferred to entities in third countries. Long story short, complementing DP Agreements with data transfer mechanisms has an added value. This added value rests with the fact that these provisions aim to set out some additional, mainly procedural mechanisms for making the applicable data protection rules effective.

6.3.3. Transfer of Data from EEA Controllers to non-EEA Controllers

Let's now move to scenarios 3 and 4, which entail the transfer of data from an EEA data controller to a non-EEA data controller. It should first be recalled that, unlike controller-processor

agreements between public bodies falling under Articles 46(2)(a) or 46(3)(b) GDPR in order to ensure that the level of protection is not undermined once data leave the EU. Besides setting out their scope and containing the definition of some basic data protection concepts, international agreements shall ensure (i) that both parties comply with the core data protection principles; (ii) that data protection rights are made enforceable and effective; (iii) that onward transfer is generally restricted; (iv) that additional safeguards are implemented when sensitive data are transferred; (v) that redress mechanisms are in place; (vi) that the proper application of the international agreement is subject to internal (e.g., periodic internal checks) and external supervision. See, 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 - Version 1.0*.

transfers, the non-EEA controllers will gain a certain freedom in determining how and for what purposes the transferred data should be processed. Indeed, while processors, regardless of their physical location, are bound to process data solely on the basis of the instructions of the data controller who will hence retain control over the transferred data, when data are transferred to a non-EEA controller, such entity will gain autonomous decision-making powers over the processing of the data. Before moving forward in the analysis, it should also be kept in mind that, unlike controller-processor relationships, when data are transferred from an EEA controller to another EEA controller, the GDPR does not require the implementation of any specific arrangement or agreement.[1179]

As a further premise, it is worth highlighting that, if the proposed jurisdictional approach is to be followed (and, as a result of this approach, data transfer mechanisms are not implemented when data are transferred to non-EEA data controllers that are directly subject to the GDPR), its actual application may raise some practical problems. First and foremost, as seen in Chapter 3, several legal uncertainties still affect the boundaries of the territorial scope of the GDPR. This entails that establishing when a non-EEA data controller is directly subject to the GDPR with the view of determining whether data transfer provisions should be implemented or not may be highly challenging. Making the implementation of data transfer provisions dependant on whether the non-EEA data recipient is directly subject to the GDPR or not would hence transpose the legal uncertainties affecting the territorial scope of the GDPR to the implementation of data transfer provisions.

Secondly, both legal and practical problems remain in the event of onward transfers. The third-country data controller (recipient A) to which data would be transferred without implementing data transfer provisions (because recipient A is directly subject to the GDPR) may then transfer the same

[1179] Specific requirements are instead prescribed by Article 26 GDPR for joint controllers. Indeed, pursuant to Article 26, joint controllers "shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an *arrangement between them* unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject" (italics mine). On this point, see Piotr Foitzik, "How to Comply with Provisions on Joint Controllers under the GDPR," *Iapp*, September 26, 2017, accessed February 11, 2019, https://iapp.org/news/a/how-to-comply-with-provisions-on-joint-controllers-under-the-gdpr/.

data to another organization (recipient B) in another country or even in the same country. If recipient B, regardless of its location, is not subject to the GDPR, data transfer provisions would need to be complied with. Following this logic, data transfer provisions would need to be implemented when data are transferred from recipient A to recipient B even if both recipients are located in the same country, but they are subject to different data protection legislations. In this respect, it can be argued that the application of GDPR data transfer provisions, which clearly entail a transfer of data across borders, to data transfers within the same country "might require a certain twist of logic".[1180]

Another scenario may raise some further, unanswered, questions: the non-EEA data controller ceases to be subject to the GDPR but still retains the transferred data. This may occur, for example, when the non-EEA data recipient starts processing the transferred data for activities that are related neither to the offering of goods or services to data subjects in the European Union nor to the monitoring of their behaviour. A restricted transfer would so occur even if data are *not* transferred from one controller to another. Ensuring continued compliance with the GDPR in a similar scenario where the original data recipient stops being directly subject to the GDPR – thus originating a situation where data transfer provisions should be, but were not, originally implemented – is bound to be a challenging task.[1181]

Leaving aside the practical problems that may arise from the application of the proposed jurisdictional approach, or at least from the application of such approach without some fine-tuning, let's now move to the analysis of scenarios 3 and 4. Once again, this analysis should be conducted in

[1180] David Smith, "ICO Brings Some Welcome Clarification to the GDPR's International Transfer Rules," *Allen & Overy - Digital Hub*, September 7, 2018, accessed February 10, 2019, http://aodigitalhub.com/2018/09/07/ico-brings-some-welcome-clarification-to-the-gdprs-international-transfer-rules/. Smith, however, argued that this "twist of logic" "may well be a small price to pay if businesses are to benefit from what seems to be a sensible and proportionate approach to interpreting and applying the GDPR in this challenging area".

[1181] Ibid. Smith noted that: "[w]hilst it might require a necessary twist of logic to conclude that a restricted international transfer takes place when a non-EU controller, subject to the GDPR, makes a transfer to another non-EU controller in the same country, albeit one not caught by the GDPR, it arguably requires a rather more substantial mental gymnastics to conclude that a restricted international transfer is also taking place when the processing of personal data leaves the scope of the GDPR without the data even being transferred from one controller to another, let alone moved across any border. There is also a more practical question of how, in such circumstances, the controller could be expected to satisfy the international transfer restrictions in Chapter V, other than by obtaining the data subject's explicit consent, as it clearly will not be in a position to enter into contractual clauses with itself".

the light of the two criteria that should be taken as a benchmark when assessing whether a data protection system or other safeguards provide for adequate protection: (1) content principles, and (2) procedural/enforcement mechanisms.

Let's start with scenario 3, which entails transfer of data from an EEA data controller to a non-EEA data controller which is *not* directly subject to the GDPR. It is clear in this case that it is "not possible to rely on the continued automatic applicability" of the EU data protection principles[1182] since the data exporter will, to a great extent, relinquish control over such data to the non-EEA data controller. The implementation of data transfer mechanisms in scenario 3 seems hence particularly compelling in order to ensure the applicability of the basic EU content principles to the processing activities conducted by the non-EEA data controller (first requirement). Indeed, in the absence of any arrangement that, along the lines of DP Agreements, determine how data should be processed by the data recipient, there is no guarantee that the non-EEA data recipient will abide by the EU data protection rules, unless some other safeguards (i.e., data transfer mechanisms) are implemented. This is mirrored in the 2001 and 2004 SCCs for controller-controller data transfers under which, unlike 2010 SCCs, the data importer specifically undertakes to process the transferred data in accordance with the data processing principles set forth in the annexes to the SCCs.[1183] The implementation of data transfer mechanisms would also be necessary in order to ensure the enforceability and hence the effectiveness of the (applicable) data protection rules (second requirement). The need to implement data transfer provisions when data are transferred to non-EEA data controllers that are not subject to the GDPR is hence beyond doubts.

Let's now move to scenario 4: transfer of data from an EEA data controller to a non-EEA data controller which is directly subject to the GDPR. In this scenario, the rules on applicable law set out under Article 3 GDPR certainly satisfy the first requirement, i.e., ensuring that the basic data protection rules apply to the processing of the transferred data. Indeed, when the non-EEA data

[1182] Article 29 Data Protection Working Party, *WP12*, 19.

[1183] Clause 5(b) 2001 SCCs and Clause II(h)(iii) 2004 SCCs. See also, Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*, 191.

recipient is directly subject to the GDPR, the EU data protection rules will be applicable to the relevant processing activities simply by virtue of the broad (extra)territorial scope of the Regulation so that no further undertaking to abide by such rules on the part of the data recipient would be necessary. In the light of this, it could be argued that implementing data transfer provisions with the view of ensuring that the data recipient is subject to the EU data protection rules would be superfluous.[1184]

At the same time, however, and keeping in mind the enforcement problems that arise from a unilateral extra-territorial expansion of the EU jurisdiction (3.6.), data transfer provisions may translate into an *indirect* way of ensuring the *effective* implementation of the GDPR or, at least, of its basic principles.[1185] Indeed, the implementation of data transfer provisions would complement, and hence strengthen, the direct (but *weak*) applicability of the GDPR with some additional provisions (included either in standard contractual clauses or in binding corporate rules or in adequacy decisions or in other legal bases for transfer) aimed at ensuring that at least some basic data protection principles are not only applicable but also made effective by means of specific enforcement and procedural mechanisms.[1186] In other words, just like DP Agreements seem to be *fit* for ensuring the applicability of the basic data protection principles (first requirement) but *unfit* for ensuring the enforcement of such principles, Article 3 GDPR certainly expands the applicability of the Regulation to non-EEA data controllers, but it seems unable to fulfil *per se* the second requirement (i.e., procedural/enforcement mechanisms).

In order to understand to what extent data transfer mechanisms adds an extra layer of protection to the transferred data, let's consider 2001 and 2004 SCCs for controller-controller transfers. Along the lines of 2010 SCCs for controller-processor transfers, both 2001 and 2004 SCCs include third-party beneficiary clauses under which data subjects are entitled to enforce several

[1184] As seen above, 2001 SCCs, 2004 SCCs, and BCRs include the data protection principles to be observed by the data recipient or by the BCR members.

[1185] Article 3 GDPR imposes on non-EEA entities full compliance with the Regulation, while data transfer provisions aim to make sure that the "basic" data protection principles are complied with by the non-EEA data recipient.

[1186] Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation," 136.

clauses against both parties to the contract.[1187] One could argue that even in the absence of similar clauses, and by virtue of the general applicability of the GDPR, data subjects would be entitled to enforce their rights against the data importer in the event of an infringement of the Regulation. Following this logic, however, data subjects would be burdened with the task of enforcing their rights against a non-EEA data controller which may be established in a country with no institutional mechanisms that allow complaints to be investigated and with no mechanisms that provide data subjects with appropriate support in the exercise of their rights.

To make things worse, unlike controller-processor transfers where the data controller continues to exercise control over the transferred data and to be responsible for ensuring compliance of its processor's activities, in controller-controller transfers it is not possible to rely on the "continued liability for damages of the transferer of the data" since, in transferring data to another controller, the data transferer loses control over the processing of those data.[1188] In other words, in the absence of a specific commitment by the data exporter to be liable for the damages that result from breaches by the data importer, there would be no legal ground under the GDPR for data subjects to enforce their rights against the EEA data exporter. This is precisely the gap that SCCs aim to fill. Under clause 6 of 2001 SCCs, in fact, the data exporter and the data importer agree to be *jointly and severally liable* for damages caused to the data subjects as a result of the violations of the provisions under SCCs. In commenting on this liability regime as set out in the draft Commission decision on 2001 SCCs, the A29WP stressed that

> joint and several liability of the data exporter and the data importer vis a vis the data subject of any damages resulting from the violation of the standard contractual clauses, is the only way to address, in a efficient and realistic manner, the serious difficulties that the contractual solution poses for the enforcement of individuals' rights and proper compensation for damages.[1189]

At the same time, the A29WP also recognized that the "joint and several liability" regime is not the only acceptable system of liability. Alternative systems of liability can also be explored as long as

[1187] Clause 3, 2001 SCCs and Clause III, 2004 SCCs.
[1188] Article 29 Data Protection Working Party, *WP12*, 19.
[1189] Article 29 Data Protection Working Party, *WP38*, 6.

"individuals are provided with readily means to exercise third party beneficiary rights and get appropriate compensation in case of damages".[1190] In other words, means are less important than results.

An alternative system of liability was, indeed, developed in 2004 SCCs, under which the data exporter and the data importer are not jointly and severally liable vis-à-vis data subjects, but they are "only" liable for their respective breach of their contractual obligations. At the same time, however, 2004 SCCs provide for a *greater involvement* of the data exporter in addressing data subject's complaints since in cases "involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer" and "if the data exporter does not take such action within a reasonable period ..., the data subject may then enforce his rights against the data importer directly".[1191] Moreover, data subjects are also "entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations" under the clauses (*culpa in eligendo*).[1192] The data exporter shall, in fact, undertake to use "reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses" by conducting audits on the premises of the data importer and by requesting evidence of the fact that the data importer has sufficient assets to fulfil its responsibilities.[1193] As a further means to facilitate the enforcement of data subjects' rights, the data importer shall also accept to be sued by data subjects in the jurisdiction of the data exporter's country of establishment.[1194] These latter undertakings are particularly relevant in ensuring the enforceability of data subjects' rights. Indeed, the right to obtain redress would be meaningless if the data importer has no sufficient financial resources to cover the payment of compensation or if data subjects would be required to sue the data importer in its country of

[1190] Article 29 Data Protection Working Party, *Opinion 8/2003 on the Draft Standard Contractual Clauses Submitted by a Group of Business Associations ("the Alternative Model Contract") (WP84)*, 2003, 6, accessed January 6, 2020, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp84_en.pdf.

[1191] Clause III(b) 2004 SCCs.

[1192] Clause III(b) 2004 SCCs. See also Recital 5, Commission decision 2004/915/EC.

[1193] Clause I(b) 2004 SCCs. See also Recital 5, Commission decision 2004/915/EC.

[1194] Clause III(b) 2004 SCCs. See also Recital 6, Commission decision 2004/915/EC.

establishment where institutional mechanisms allowing complaints to be investigated and compensation to be paid may not be in place.

As for the duties of cooperation with DPAs, under both sets of clauses, and in line with 2010 SCCs, the data importer undertakes to cooperate with the competent data protection authority and to submit its data processing facilities for audit.[1195] This specific undertaking may be regarded as unnecessary when the data recipient is directly subject to the GDPR. Indeed, under Article 31 GDPR, the "controller ... shall cooperate, on request, with the supervisory authority in the performance of its tasks". Thus, as a normative matter, there would be no need to "contractually" expand DPA's monitoring and investigative powers. DPAs would, in fact, gain these (extended) powers through the direct applicability of the GDPR, and of Article 31 more specifically.

To the contrary, despite the direct applicability of the GDPR to non-EEA data controller, the problem of overriding laws would remain: even if the non-EEA data controller is bound to process the transferred data in compliance with the GDPR, there is no guarantee that the third country's law to which the non-EEA entity is subject will provide for limitations to the public authorities' ability to access data. This is why, in line with 2010 SCCs, under Clause 5(a) of 2001 SCCs and, equally, under Clause II(c) of 2004 SCCs, the data importer warrants that it has no reason to believe that the legislation to which it is subject prevents it from fulfilling the obligations under the contract and that it will inform the data exporter and the competent supervisory authority in the event of a change in the legislation which may have substantial adverse effect on the guarantees provided for under the contract.[1196] The competent data protection authorities also have the power to prohibit or suspend data flow so as to protect individuals with regard to the processing of their personal data.[1197]

[1195] Clause 5(d) Clause 8 2001 SCCs.

[1196] Clause 5(a) 2001 SCCs and Clause II(c) 2004 SCCs.

[1197] See Article 4 Commission Decision 2001/497/EC as amended by European Commission, *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*.

The same considerations can be extended to the other data transfer mechanisms. As seen above (6.3.2.), in fact, BCRs do not only include a provision that ensures that basic data protection principles apply throughout the corporate group (provision that would be made superfluous by Article 3), but they also set out a system of enforcement safeguards. Among others, third-party beneficiary rights and the acceptance by the EEA headquarter (or other BCR member) of responsibility for any breach of any non-EEA data importer; a complaint handling process; training programs; self-audits as well as acceptance to be audited by DPAs; and information requirements in the event of requests for disclosure of personal data by third countries' public authorities. Equally, under adequacy decisions, the European Commission establishes not only that the third countries to which data are transferred provide for "adequate" data protection rules (assessment which, again, would be made superfluous by Article 3) but also that mechanisms for regulatory oversight and for judicial or administrative redress have been established.

6.3.4. Filling the Gap between the Applicability of Data Protection Rules and their Effective Implementation

The previous sections have discussed to what extent, rules on applicable law can sufficiently and effectively achieve the objective(s) underpinning data transfer provisions and, ultimately, replace such rules. It has been argued that in order to understand the added value, if any, of implementing data transfer provisions when the data recipient is already directly (when data are transferred to non-EEA controllers that are caught under Article 3 GDPR) or indirectly (when data are transferred to non-EEA data processors which are contractually bound to follow the EEA controller's instructions by virtue of the DP Agreement) subject to the GDPR, two basic elements should be taken into considerations: (1) the content of the rules applicable to the processing activities conducted by the data recipient; (2) the procedural/enforcement mechanisms for making such rules effective. As it has been highlighted above, these are the two requirements to be considered when assessing the adequacy of a system (under Article 45 GDPR) or of other safeguards (under Article 46 GDPR) in protecting transferred data. In other words, in the view of the A29WP, the applicability of data protection rules

does not provide *per se* adequate protection to the transferred data (first requirement) if it is not complemented with instruments that make such applicable rules effective (second requirement). After all, "data protection rules only contribute to the protection of individuals if they are followed in practice".[1198] Moreover, in WP254, the A29WP has also added a *third* element that should be considered when assessing the adequacy of the level of protection offered by a third country, i.e., that essential guarantees are in place for limiting access to data for law enforcement and national security reasons. This reflects the problem of overriding law that affect contractual solutions.

The analysis conducted above has shown that even if the *applicability* of the EU data protection principles to the processing activities conducted by the non-EEA data recipient seems to be ensured by Article 3 GDPR (in scenario 4) and by DP Agreements (in scenarios 1 and 2), international data transfers still raise specific challenges compared to intra-EEA transfers: ensuring the enforceability of the applicable rules by both data protection authorities and data subjects, and the problem of overriding law. And data transfer mechanisms, however time-consuming and often merely formalistic,[1199] represent an *attempt* to deal with such challenges. Here lies the added value of implementing data transfer provisions even when the data recipient is, directly or indirectly, subject to the GDPR. Indeed, given that the applicability of legislation does not always guarantee its effective implementation,[1200] the existing data transfer mechanisms do not only address the general data protection principles that should be implemented in the processing of the transferred data but also how regulatory oversight can be ensured and how redress can be guaranteed to data subjects.

[1198] Article 29 Data Protection Working Party, *WP12*, 5.

[1199] For example, dealing with audit rights in contracts is often impractical considering the administrative burdens that the data importers would need to bear to allow their (often numerous) customers to exercise their on-premise audit rights and the security issues that may derive from these audits. Centre for Information Policy Leadership, *Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR*, 11. Moreover, audits and investigations by national DPAs in the territory of another State contravenes one of the basic rules of international law which prohibits the authorities of one State from carrying out acts in the territory of another State. At the same time, there are some cases involving audits by EU DPAs outside their own territory. On this point, see Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law," 239–240; Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)," 232–234.

[1200] Joseph Alhadeff, Brendan Van Alsenoy, and Jos Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," in *Managing Privacy through Accountability*, ed. Daniel Guagnin et al. (London: Palgrave Macmillan, 2012), 82.

In the light of the above, it could be concluded that the need to implement data transfer mechanisms would become less compelling if a system a mutual cooperation is established between EEA and non-EEA supervisory authorities. A system of mutual cooperation would, indeed, help bridge the gap between the applicability of data protection principles and its effective implementation.[1201] Notably, as seen above (6.2.2.3.), international cooperation would be necessary even if solution 1 is achieved, and hence even if internationally agreed data protection standards are adopted. Indeed, arguably, the harmonization of data protection standards at the international level would meet the first requirement but would leave the second requirement unsatisfied if such standards are not complemented with cross-border cooperation.

In this regard, it should be noted that, in Recital 116 GDPR, the EU legislators have recognized the need to promote cross-border cooperation between supervisory authorities as a means to address the enforcement problems that may arise when data are transferred to third countries:

> … there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.[1202]

Article 50 GDPR is moving in this direction. Indeed, this article prescribes that the Commission and supervisory authorities shall take steps in order to facilitate the effective enforcement of data protection legislation by developing international cooperation mechanisms; to provide international mutual assistance in enforcing data protection rules, "including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms"; to engage stakeholders in discussions "aimed at furthering international cooperation in the enforcement of legislation for the

[1201] Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 2)," 243.
[1202] Recital 116 GDPR.

protection of personal data"; to promote information sharing "including on jurisdictional conflicts with third countries".[1203]

As noted by the European Commission in its 2017 Communication to the European Parliament and the Council, Article 50 GDPR recognizes the importance of international cooperation between supervisory authorities as a means not only to make protection of personal data more effective but also to create more legal certainty for economic operators.[1204] The modern digital economy is, in fact, populated by companies that increasingly act on a global level and that hence process a vast amount of data from people in more than one jurisdiction. This entails that "problems of noncompliance with data protection rules or data breaches simultaneously affect people in more than one jurisdiction" thus increasing the need for developing cooperation mechanisms with international partners. The European Commission also noted that important lessons on how to boost effective enforcement can be learned from other areas of law, such as competition and consumer protection.[1205]

Some frameworks of international cooperation have already been established with the aim of supporting and facilitating the enforcement of data protection laws. As mentioned above (6.2.2.3.), an essential role is played in this regard by the Council of Europe. Indeed, Convention 108 sets forth a framework for mutual assistance between national authorities in implementing the data protection rules set out under the Convention.[1206] Issues of cooperation are also addressed in the modernized Convention 108 under which the "Parties agree to co-operate and render each other mutual assistance in order to implement this Convention",[1207] in particular, by exchanging information,[1208] by "co-ordinating their investigations or interventions, or conducting joint actions",[1209] and by "providing information and documentation on their law and administrative practice relating to data

[1203] Article 50, GDPR.
[1204] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 5.
[1205] Ibid., 12–13.
[1206] Chapter IV, Convention 108 ("Mutual assistance").
[1207] Article 16(1) Convention 108 +.
[1208] Article 17(1)(a) Convention 108 +.
[1209] Article 17(1)(b) Convention 108 +.

protection".[1210] Moreover, in order to perform their cooperation duties, "the supervisory authorities of the Parties shall form a network"[1211] as a means to rationalise the cooperation process and hence to boost the efficiency of the protection of personal data.[1212] Since Convention 108 is open to accession by both European and non-European States, the framework for international cooperation detailed in Convention 108, in both the old and the modernized versions, has the potential of setting the ground for a *global* system of mutual cooperation.[1213]

The need to boost international cooperation between supervisory authorities is also an issue of concern for the OECD. Indeed, in 2006, the OECD issued a report on the cross-border enforcement of privacy laws where it analysed the challenges that enforcement authorities face in addressing cross-border cases. In this report, it acknowledged the fact that existing international frameworks for facilitating cross-border cooperation are not "sufficiently comprehensive or globally co-ordinated to adequately address the cross-border enforcement challenges".[1214] Following this report, in 2007, the OECD issued a recommendation on cross-border cooperation in the enforcement of laws protecting privacy, where it recommended that Member countries take steps to

> a) Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.
> b) Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.
> c) Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.
> d) Engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.[1215]

[1210] Article 17(1)(c) Convention 108 +.
[1211] Article 17(3) Convention 108 +.
[1212] Council of Europe, *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, paragraph 143.
[1213] Dariusz Kloza and Anna Mościbroda, "Making the Case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insights from Competition Law," *International Data Privacy Law* 4, no. 2 (May 1, 2014): 129.
[1214] Organisation for Economic Cooperation and Development, *Report on the Cross-Border Enforcement of Privacy Laws*, 4.
[1215] Organisation for Economic Cooperation and Development, *Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy*, 7.

As a means to foster mutual assistance, the OECD also called for Member countries to establish an informal network of enforcement authorities to discuss practical aspects of the cross-border enforcement cooperation, to share best practices, to develop shared enforcement priorities, and to support joint enforcement initiatives.[1216] Building upon this recommendation, in 2008, data protection authorities started to share their experience and to discuss practical aspects of cooperation in cross-border cases. Two years later, eleven privacy authorities launched the Global Privacy Enforcement Network which was later joined by sixteen additional authorities. The mission of this network is to connect "privacy enforcement authorities from around the world to promote and support cooperation in cross-border enforcement of laws protecting privacy", in particular by exchanging information, good practices and expertise, and by creating mechanisms or processes useful for international cooperation.[1217]

Another important framework for boosting international cooperation among enforcement authorities is the ICDPPC which gathers 122 data protection authorities from all over the world. The ICDPPC has adopted several, mainly advisory and hence non-legally binding resolutions in which it urged DPAs to enhance international cooperation which has become one of the major focus of the conference.[1218] The Madrid resolution adopted by the 31st ICDPPC in 2009 (6.2.1.) merits special attention in this regard. Indeed, after prescribing that "[i]n every State there shall be one or more supervisory authorities, in accordance with its domestic law, that will be responsible for supervising the observance of the principles set out" in the Resolution,[1219] it also provides that such supervisory authorities "shall try to cooperate with each other to achieve a more uniform protection of privacy with regard to the processing of personal data, at both national and international level". In particular, supervisory authorities shall share reports, investigation techniques, and other useful information

[1216] Ibid., paragraph 21.

[1217] Global Privacy Enforcement Network, *Action Plan for the Global Privacy Enforcement Network*, 2012, accessed April 15, 2019, https://www.privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen.

[1218] For an overview of the relevant resolutions adopted by the ICDPPC see, Kloza and Mościbroda, "Making the Case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insights from Competition Law," 122–123.

[1219] Article 23, Madrid Resolution.

especially "following a request for cooperation by another supervisory authority"; they shall "[c]onduct co-ordinated investigations or interventions, at both national and international level" and take part to joint fora in order to contribute to the adoption of joint positions.[1220]

Moreover, in 2017, the ICDPPC has established the Working Group on International Enforcement Cooperation (WGIEC) which was mandated to "explore the feasibility of potential framework options that may facilitate a broader geographic and functional scope of cooperation of privacy enforcement cooperation".[1221] In keeping with this mandate, the WGIEC presented to the 41th Conference the results of its study on the possible legal solutions for international enforcement cooperation: (1) the addition of a legally binding schedule to the Global Cross-border Enforcement Cooperation Arrangement which was adopted in 2014 and that aims to facilitate enforcement cooperation between members; (2) the possibility of developing a set of model contract clauses or of bilateral or multilateral agreements that national DPAs may use to cooperate; (3) the possibility of framing privacy enforcement cooperation under an international mutual legal assistance treaty.[1222] The importance of enforcement cooperation was reiterated by the 41st ICDPPC in its 2019-2021 policy strategy in which it recognized that the international flow of personal data has made international enforcement cooperation an essential component for promoting data protection both domestically and globally.[1223]

Other arrangements have been established at the regional level. Within the APEC region, for example, the Cross-border Privacy Enforcement Arrangement (CPEA) was established in 2010 with the aim of building an arrangement for (voluntary) cooperation between the enforcement authorities

[1220] Article 24, Madrid Resolution.

[1221] 39th International Conference of Data Protection and Privacy Commissioners, *Resolution on Exploring Future Options for International Enforcement Cooperation* (Hong Kong, 2017), 4, accessed December 22, 2019, http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-exploring-future-options-for-International-Enforcement-Cooperation-2017.pdf.

[1222] Working Group on International Enforcement Cooperation, *Final Report - 41st International Conference for Data Protection and Privacy Commissioners*, 2019, accessed December 22, 2019, https://privacyconference2019.info/wp-content/uploads/2019/11/ICDPPC-WGIEC-Final-Report-October-2019-published-final-1.pdf.

[1223] 41st International Conference of Data Protection and Privacy Commissioners, *Resolution on the Conference's Strategic Direction (2019-21)*, 7–8.

in APEC economies (6.4.2.4.).[1224] Other examples include the Asia Pacific Privacy Forum,[1225] the Ibero-American Data Protection Network,[1226] the French-speaking Association of Personal Data Protection Authorities,[1227] and the Central and Eastern European Data Protection Authorities.[1228] Other forms of international cooperation have also been established on a bilateral level, for example between the Spanish DPA and the US Federal Trade Commission (2005), between Australia and New Zealand (2008), between Germany and Canada (2012), and between the Dutch and the Canadian DPAs, which in 2011 signed a Memorandum of Understanding in order to coordinate their (joint) investigation into WhatsApp privacy policy.[1229] The official website of the Canadian DPA lists all the written arrangements that the Canadian DPA has signed with its counterparts from other countries (Dubai, Germany, Ireland, The Netherlands, Romania, United Kingdom, and Uruguay).[1230]

It is clear from the above that several international frameworks have been established both on multilateral and bilateral levels for enhancing and supporting cooperation between DPAs in cross-border cases. However, the list of the instruments analysed above is mainly composed of either non-binding or non-comprehensive arrangements. Indeed, most of the fora for international cooperation that are currently available mainly establish voluntary and informal networks and/or are limited to some specific jurisdictions or regions. Convention 108 is the only instrument that offers the tools for (potentially) tackling privacy breaches on a global scale since it includes both comprehensive and

[1224] APEC, *Cooperation Arrangement Cross-Border Privacy Enforcement* (Hiroshima, Japan: 2010/SOM1/ECSG/DPS/013, 2010), accessed April 15, 2019, http://mddb.apec.org/documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf. As clarified under paragraph 6.2. of the Cooperation Arrangement, "[n]othing in this Cooperation Arrangement is intended to: (i) Create binding obligations, or affect existing obligations under international or domestic law, or create obligations under the laws of the Participants' economies".

[1225] Asia Pacific Privacy Forum, http://www.appaforum.org/.

[1226] Ibero-American Data Protection Network, http://www.redipd.es/index-ides-idphp.php.

[1227] French-speaking Association of Personal Data Protection Authorities, https://www.afapdp.org/.

[1228] Central and Eastern European Data Protection Authorities, http://www.ceecprivacy.org/main.php.

[1229] *Memorandum of Understanding between the Privacy Commissioner of Canada and College Bescherming Persoonsgegevens on Mutual Assistance in the Enforcement of Laws Protecting Personal Information in Private Sector*, 2011, accessed April 15, 2019, https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-memorandums-of-understanding/mou-netherland/. For an overview of the arrangements for international cooperation on a bilateral level, see Kloza and Mościbroda, "Making the Case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insights from Competition Law," 123–124.

[1230] Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-memorandums-of-understanding/.

binding provisions.[1231] This conclusion is confirmed by the PHAEDRA I project, a two-year project launched in 2013 with the funding of the European Commission and aimed at improving cooperation between DPAs around the world.[1232] One of the main findings of the project is that, even if cooperation and coordination mechanisms exist at multiple levels, they are not effective as they could be.[1233] At the same time, there is "good evidence of a clear desire for increased co-operation and co-ordination enforcement, as well as information sharing between DPAs".[1234]

Against this background, it can be concluded that the possibilities for cross-border cooperation between DPAs should be increased. This may require States to amend their internal laws in order to allow their DPAs to engage in these forms of international cooperation.[1235] For example, the Working Group on International Enforcement Cooperation observed that the model contractual clauses may not be a feasible solution for establishing international cooperation between national DPAs since in some jurisdictions national DPAs do not have the ability to enter into legally binding agreements with other authorities. For these members, the ability to enter into such agreements is reserved to governmental bodies.[1236]

The appointment of a representative in the EU as required by Article 27 GDPR (3.6.) may, to some extent, help filling the gap between the applicability and the enforceability of data protection law. Indeed, the role of representatives is to establish a liaison between EU DPAs and data subjects in the EU on the one hand, and the non-EU data controller or processor that they represent on the other. At the same time, however, as clarified by the EDPB, the "GDPR does not establish a

[1231] Kloza and Mościbroda, "Making the Case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insights from Competition Law," 125 and 135–138.

[1232] PHEADRA I project (2013-2015) was aimed at making recommendations on how to improve DPA's cooperation on a global scale, while PHAEDRA II (2015-2017) focused on how to improve cooperation between DPAs within the EU. PHAEDRA stands for "Improving Practical and Helpful cooperAtion bEtween Data pRotection Authorities".

[1233] PHAEDRA, *Co-Ordination and Co-Operation between Data Protection Authorities*, 2014, 170–172, accessed April 15, 2019, http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf.

[1234] Ibid., 171.

[1235] Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, 41.

[1236] Working Group on International Enforcement Cooperation, *Final Report - 41st International Conference for Data Protection and Privacy Commissioners*, 20–22.

substitutive liability of the representative in place of the controller or processor it represents in the Union".[1237] This entails that the EU DPAs may still be required to take actions against the non-EU entity and hence to engage in international cooperation with non-EU data protection authorities.

6.4. Solution 3: Solving Data Transfer Issues by Means of the Accountability Principle

6.4.1. Scope of the Section

The difficulties of overcoming the limitations of data transfer mechanisms as they are currently designed under Chapter V of the GDPR and the shortcomings of the possible paths forward identified and analysed above suggest that more innovative solutions should be explored. This section hence aims to identify the possible foundations for a new data transfer regime building on the concept of "accountability" as it has been developed not only within the EU framework but also in other jurisdictions, namely in the Asia-Pacific Economic Cooperation (APEC) and in Canada under the Personal Information Protection and Electronic Documents Act (PIPEDA)[1238]. The accountability principle is not new but it has received a growing attention in recent years as a means to increase *organizational responsibility* in ensuring appropriate safeguards when processing personal data.[1239] As it will be argued below, the development of an accountability-based data transfer regime is preferable (as well as feasible) since it acknowledges the inherent limits of the existing data transfer tools in achieving their underlying objectives by increasing companies' responsibility to adequately and proactively safeguard the data in their care. This *increased onus on companies* in ensuring compliance with the applicable data protection principles would hence push most of the burden for ensuring compliance with the EU data protection standards on the companies concerned and away from regulators.[1240]

[1237] European Data Protection Board, *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 27.

[1238] *Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)* (S.C. 2000, c. 5, 2000).

[1239] Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 105–106.

[1240] Information Integrity Solutions, *Towards a Truly Global Framework for Personal Information Transfers. Comparison and Assessment of EU BCR and APEC CBPR Systems*, 2013, 31, accessed July 27, 2019,

This section will hence begin with a tentative definition of the principle of accountability followed by an overview of the different nuances which the said principle takes in the various (national, supranational and international) data protection contexts in which it was developed. Drawing from this analysis, the second part of this section aims to identify the elements which should be valued and further developed as building blocks for a data transfer framework based on the principle of accountability. The existing accountability-based data transfer tools seem, indeed, to include some promising components which could inform the development of a more effective, more scalable, more predictable and at the same time more flexible framework for international data transfers.

6.4.2. The Accountability Principle within and outside the EU Framework

6.4.2.1. Defining "Accountability"

The starting point of the analysis on the accountability principle in the data protection field necessarily starts from the definition of the term "accountability". The Oxford English Dictionary defines "accountability" as "[t]he quality of being accountable; liability to account for and answer for one's conduct, performance of duties, etc. (in modern use often with regard to parliamentary, corporate, or financial liability to the public, shareholders, etc.); responsibility".[1241] The definition of "accountable" given by the same dictionary is being "liable to be called to account or to answer for responsibilities and conduct; required or expected to justify one's actions, decisions, etc.; answerable, responsible".[1242] It is hence clear from these definitions that accountability and responsibility go hand-in-hand: being accountable means being liable to be called to answer for one's responsibility. The necessary involvement of an external body also emerges from these definitions. As explained by Bennett (2010), "[a]ccountability implies a process of transparent interaction, in which that [external]

https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f628a8a65e232a6959b80/1465868951114/IIS+CBPR-BCR+report+FINAL.pdf.

[1241] *Oxford English Dictionary*, 3rd ed., 2011.

[1242] Ibid.

body seeks answers and possible rectification".[1243] Accountability is hence strongly connected to responsibility but, at the same time, it is something more than responsibility since, unlike responsibility, accountability always entails reference to an external agent.[1244] The analysis that will be conducted below will highlight the different nuances that the principle of accountability acquires in the various data protection contexts in which it was developed.

6.4.2.2. OECD Guidelines and Madrid Resolution

As mentioned above, the accountability principle, as a data protection principle, has been developed in different contexts, both within and outside the EU, both at the national and supranational/international levels. The accountability principle made its debut in the data protection arena in the 1980 OECD Guidelines. Under the said Guidelines, the principle of accountability provides that a "data controller should be accountable for complying with measures which give effect to" the other data protection principles listed in the Guidelines.[1245] The role of the principle of accountability is hence to ensure that the principles enshrined in the OECD Guidelines are implemented in practice. The Explanatory Memorandum of the 1980 OECD Guidelines explains the rationale behind the principle in question as follows:

> The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly. it is essential that under domestic law *accountability for complying with privacy protection rules and decisions should be placed on the data controller* who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel ... and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information ... Accountability ... refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.[1246]

[1243] Colin Bennett, "International Privacy Standards: Can Accountability Be Adequate?," *Privacy Laws & Business International Newsletter*, no. 106 (August 2010): 21, accessed August 21, 2019, https://dspace.library.uvic.ca/bitstream/handle/1828/10394/Bennett_Colin_PrivLawsBusiness_Aug%202010.pdf?sequence=1.

[1244] Ibid.

[1245] Paragraph 14, 1980 OECD Guidelines.

[1246] Paragraph 62 (italics mine), *Explanatory Memorandum*, 1980 OECD Guidelines.

It is clear from the explanation above that the principle of accountability, as worded under the OECD Guidelines, mainly aims to identify the data controller as the entity (primarily) responsible for ensuring compliance with the applicable data protection principles and hence as the entity which may be called to answer for its responsibilities in case of non-compliance. Moreover, the explanatory memorandum clarifies that the data controller should not be relieved from this responsibility merely because the data processing is conducted by a third party on his behalf, presumably not even when such third party is located in a foreign jurisdiction.[1247]

The principle of accountability under the 1980 version of the OECD Guidelines is hence mainly serving the purpose of allocating primary responsibility for complying with the relevant data protection principle upon the data controller. Apart from a quick reference to legal sanctions and codes of conducts in the Explanatory Memorandum, little attention is instead placed on the *means* to implement and demonstrate accountability. This gap was however filled in the updated 2013 version of the Guidelines. Indeed, building on the increasing attention that the principle of accountability has received in recent years as a means to foster organizational responsibility, the revised OECD Guidelines have introduced a new section (part three) on "Implementing Accountability". Under the said section,

> A data controller should:
> a) Have in place a privacy management programme that:
> i. gives effect to these Guidelines for all personal data *under its control*;
> ii. is tailored to the structure, scale, volume and sensitivity of its operations;
> iii. provides for *appropriate safeguards* based on privacy risk assessment;
> iv. is integrated into its governance structure and establishes internal oversight mechanisms;
> v. includes plans for responding to inquiries and incidents;
> vi. is updated in light of ongoing monitoring and periodic assessment.[1248]

Part three on "Implementing Accountability" hence provides that data controllers should implement a privacy management programme. This programme should be designed so as to ensure that appropriate safeguards are in place not only with reference to their own processing operations

[1247] Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 53–55.

[1248] Paragraph 15(a), 2013 OECD Guidelines (italics mine).

but "for all personal data under [their] control",[1249] even if those data are processed by third parties on their behalf and even in their relationships with other data controllers, especially if responsibility for processing is shared. Moreover, paragraph 16 of the 2013 OECD Guidelines explicitly clarifies that "[a] data controller remains accountable for personal data under its control *without regard to the location of the data*".[1250] Indeed, the transfer of data to third countries present risks which the data controller is required to address especially considering that data may be transferred to jurisdictions which lack the willingness and/or the capacity to implement and enforce appropriate safeguards in the processing of the transferred data.[1251] As explained in the Supplementary Explanatory Memorandum to the 2013 OECD Guidelines, appropriate safeguards may be provided by "provisions in contracts that address compliance with the data controller's privacy policies and practices; protocols for notifying the data controller in the event of a security breach; employee training and education; provisions for sub-contracting; and a process for conducting audits".[1252] An assessment of the risks to individuals' privacy should also be conducted so as to define safeguards appropriate to the risk.[1253]

At the same time, paragraph 15(a)(ii) of the revised Guidelines acknowledges that privacy management programs should be "tailored to the structure, scale, volume and sensitivity of its operations"[1254] thus recognizing the need for some flexibility in the determination of the programs: "[f]or example, large data controllers with locations in multiple jurisdictions may need to consider different internal oversight mechanisms than small or medium sized data controllers with a single establishment".[1255] At the same time, privacy management programs should be adapted to the volume

[1249] Paragraph 15(a)(i), 2013 OECD Guidelines.
[1250] Paragraph 16, 2013 OECD Guidelines (italics mine).
[1251] Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013), Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 30.
[1252] Ibid., 23.
[1253] Paragraph 15(a)(iii), 2013 OECD Guidelines.
[1254] Paragraph 15(a)(ii), 2013 OECD Guidelines.
[1255] Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013), Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 24.

and the sensitivity of the processing operations conducted by the data controller. Indeed, even small-sized data controllers may deal with large volumes of data or with highly sensitive data.[1256] Paragraph 15(1)(iv) also stresses the importance of incorporating privacy management programs within the controller's corporate structure: the successful implementation of such programs is indeed heavily dependent on commitments from the management, the availability of resources, and training programs.[1257] Moreover, part three on "Implementing Accountability" provides not only that data controllers should have in place a privacy management programme but also that they should be ready to *demonstrate* such programmes upon request of the competent enforcement authorities[1258] and notify such authorities and the affected data subjects in the event of a security breach.[1259]

The accountability principle was also included in the Madrid Resolution. Indeed, under Article 11 of the said Resolution, "[t]he responsible person shall: a. Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers".[1260] Like the OECD Guidelines, under the Madrid Resolution, the principle of accountability entails that the responsible person should not only implement the necessary measures to ensure compliance with the relevant data protection principles but should also demonstrate such compliance. At the same time, unlike the OECD Guidelines, the Madrid Resolution additionally clarifies that compliance should be demonstrated not only to the competent supervisory authorities but also to data subjects.[1261]

[1256] Ibid.
[1257] Ibid.
[1258] Paragraph 15 b), 2013 OECD Guidelines.
[1259] Paragraph 15 c), 2013 OECD Guidelines.
[1260] Article 11, Madrid Resolution.
[1261] Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 62.

6.4.2.3. The Canadian Experience: The Personal Information Protection and Electronic Documents Act (PIPEDA)

Moving from the international to the national level, the Canadian Fair Information Principles contained in PIPEDA also include the principle of accountability. Principle 1 on "accountability" provides that "[a]n organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with" the fair information principles.[1262] A list of the policies and practices which shall be implemented in order to give effect to the principles is also provided, including:

> (a) implementing procedures to protect personal information;
> (b) establishing procedures to receive and respond to complaints and inquiries;
> (c) training staff and communicating to staff information about the organization's policies and practices; and
> (d) developing information to explain the organization's policies and procedures.[1263]

In the light of the above, it is clear that PIPEDA refers to the principle of accountability not only to identify the entities which should be responsible for compliance with the relevant data protection rules but also for identifying the measures which are expected from those entities:[1264] "[a]n accountable organization must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws".[1265]

The principle of accountability also plays an essential role in cross-border data transfer. Indeed, clause 4.1.3 of PIPEDA clarifies that an "organization is responsible for personal information in its possession or custody, including information that has been *transferred to a third party* for processing", and hence in the event of controller-to-processor transfers. "The organization shall use contractual or other means to *provide a comparable level of protection* while the information is being

---

[1262] Clause 4.1, PIPEDA. The full text of PIPEDA is available at this link: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-11.html#h-26.

[1263] Clause 4.1.4, PIPEDA.

[1264] Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 55–56.

[1265] Office of the Privacy Commissioner of Canada, "Getting Accountability Right with a Privacy Management Program," last modified April 17, 2012, accessed August 31, 2019, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/.

processed by a third party".[1266] No distinction is hence made between domestic and international transfer as long as the transferring organization exercises due diligence in selecting the party to which data will be transferred[1267] for processing and as long as contractual safeguards are implemented so as to ensure "a comparable level of protection".[1268]

PIPEDA has hence embodied an organization-to-organization approach to data transfer rather than the state-to-state approach on which adequacy decisions, as the "preferred" EU data transfer tool, are based. Indeed, instead of focusing on the guarantees provided by the jurisdiction to which data are transferred, PIPEDA focuses on the responsibility of the transferring organizations for protecting data under their control wherever they are transferred:[1269] "PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement".[1270]

At the same time, it should be noted that, although the domestic legislation to which the data recipient is subject is not as central as under the adequacy decisions adopted within the EU framework, it still retains some relevance. Indeed, the Office of the Privacy Commissioner of Canada (OPC) recognized that "[w]hat the organization cannot do through contract - or indeed by any other means - is to override the laws of a foreign jurisdiction".[1271] This is why, before undertaking an

---

[1266] Clause 4.1.3, PIPEDA (italics mine).

[1267] "The organization must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times. It should also have the right to audit and inspect how the third party handles and stores personal information, and exercise the right to audit and inspect when warranted". Office of the Privacy Commissioner of Canada, *PIPEDA – Processing Personal Data Across Borders Guidelines*, 2009, 6, accessed August 2, 2019, https://www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf.

[1268] "'Comparable level of protection' means that the third party processor must provide protection that can be compared to the level of protection the personal information would receive if it had not been transferred. It does not mean that the protections must be the same across the board but it does mean that they should be generally equivalent". Ibid., 5.

[1269] Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 56. As explained by Kuner, "The geographically-based approach aims to protect against risks posed by the country or location to which the data are to be transferred, while the organisationally-based approach targets risks posed by the organisations which receive the data". Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, 28. The organization-to-organization approach also underpins several EU data transfer mechanisms, in particular BCRs and SCCs.

[1270] Office of the Privacy Commissioner of Canada, *PIPEDA – Processing Personal Data Across Borders Guidelines*, 4.

[1271] Ibid., 6.

international data transfer, organizations shall take into consideration all the elements surrounding the data transfer, including the foreign regime to which the third party concerned is located: "[t]he result may well be that some transfers are unwise because of the *uncertain nature of the foreign regime* or that in some cases information is so sensitive that it should not be sent to any foreign jurisdiction".[1272]

It should however be noted that the concept of "transfer" for processing has a specific meaning under PIPEDA. Indeed, transfer is intended as a "use" by the organization as opposed to "disclosure". When a company outsources the processing of data to another company (controller-to-processor transfer) data can only be processed for the purpose it was originally collected and, in this framework, consent from the data subject is not required before transfer.[1273] However, the OPC has recently revisited its interpretation of the concept of "transfer" and concluded that "the position that a transfer (i.e., when a responsible organization transfers personal information to a third party for processing) is not a 'disclosure' is debatable and likely not correct as a matter of law".[1274] The transfer from one organization to another seems, in fact, to fit perfectly within the ordinary meaning of "disclosure". This change in position by the OPC entails that organizations would be required to obtain the consent from the individuals concerned before transferring data to third parties for processing. Considering the important impact that this change is likely to have on businesses, on 9 April 2019, the OPC launched a public consultation soliciting feedback from interested parties on how the current legislation should be interpreted and applied.[1275]

[1272] Ibid., 7 (italics mine).

[1273] Ibid., 5, 9.

[1274] Office of the Privacy Commissioner of Canada, "Supplementary Discussion Document – Consultation on Transborder Dataflows," last modified June 11, 2019, accessed August 31, 2019, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/sup_tbdf_201904/.

[1275] "Organizations are free to design their operations to include flows of personal information across borders, but they must respect individuals' right to make that choice for themselves as part of the consent process. In other words, individuals cannot dictate to an organization that it must design its operations in such a way that personal information must stay in Canada (data localisation), but organizations cannot dictate to individuals that their personal information will cross borders unless, with meaningful information, they consent to this". Office of the Privacy Commissioner of Canada, "Consultation on Transborder Dataflows," last modified June 11, 2019, accessed August 31, 2019, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/.

This consultation was, however, reframed after that, in May 2019, the government released a white paper entitled "Strengthening Privacy for the Digital Age" which includes considerations for modernizing PIPEDA.[1276] In the light of this, the OPC extended the purpose of the consultation and invited stakeholders to express their opinion not only on how the current law should be interpreted but also on how a new law regulating transfer of data should be like. Notably, in the reframed consultation, the OPC has put into question the effectiveness of the principle of accountability in protecting data in the context of transborder data flow. The OPC indeed noted that the principle of accountability, as currently framed under PIPEDA, "is not always effective in protecting privacy". This mainly derive from the fact that the contractual solutions that companies are required to implement in order to "provide a comparable level of protection" are rarely subject to the scrutiny of the OPC. Such a model of "self-regulation" is deemed by the OPC "insufficient, in an age of complex technologies, data flows and business models, to give individuals the assurance and trust they need that their privacy will continue to be protected when their personal information is transferred for processing. Proactive review by an independent regulator may help provide that assurance". The OPC hence suggested that PIPEDA should "be amended to require demonstrable accountability, including an authority for the OPC to proactively inspect the practices of organizations to ensure they truly are accountable".[1277] In particular, according to the OPC, in order to add a level of review by an independent authority, a regime of standard contractual clauses, along the lines of the EU SCCs, could be adopted.[1278]

[1276] "The Government is considering how best to modernize its private-sector policy and regulatory framework in order to protect privacy and support innovation and prosperity. In short, the goal is to respect individuals and their privacy by providing them with meaningful control without creating onerous or redundant restrictions for business; enable responsible innovation on the part of organizations; and ensure an enhanced, reasoned enforcement model. Specifically, the Government is proposing clarifications under PIPEDA that detail what information individuals should receive when they provide consent; certain exceptions to consent; data mobility; deletion and withdrawal of consent; incentives for certification, codes, standards, and data trusts; enhanced powers for the Office of the Privacy Commissioner; as well certain modernizations to the structure of the law itself and various definitions". Government of Canada, "Strengthening Privacy for the Digital Age - Innovation for a Better Canada," last modified May 21, 2019, accessed August 31, 2019, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

[1277] Office of the Privacy Commissioner of Canada, "Consultation on Transfers for Processing – Reframed Discussion Document," last modified June 11, 2019, accessed August 31, 2019, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/#fn6-rf.

[1278] Ibid. The OPC also noted that another limitation of the contractual arrangements stipulated under clause 4.1.3. of PIPEDA is that they "offer limited protection against a foreign law that is inconsistent with their provisions. This

On 23 September 2019, the OPC has announced the end of the consultation. In taking into account the submissions received, the OPC concluded that the current interpretation under which companies are not required to seek data subjects' consent before engaging in cross-border transfer for processing will remain unchanged. At the same time, as a longer-term goal, the OPC will continue its efforts on how the law on cross-border transfer should be reformed so as to tackle the insufficiencies of existing privacy protections.[1279]

6.4.2.4. The APEC, the APEC Privacy Framework and the Cross-Border Privacy Rules

The accountability principle also lies at the heart of the APEC Cross-Border Privacy Rules system (CBPR). CBPR is a voluntary and certification-based regional framework for international data transfer which was promulgated in 2012 with the aim of protecting personal data throughout the APEC region[1280] without limiting their free movement. The CBPR system requires that the Economy wishing to join the system meets some specific legislative and enforcement requirements in order to receive approval from the Chair of the APEC Electronic Commerce Steering Group (ECSG). The participation criteria include the establishment of at least one Privacy Enforcement Authority (PEA) responsible for enforcing the CBPR system. PEAs belong to the Cross-Border Privacy Enforcement Arrangement (CPEA), a multilateral mechanism for PEAs to cooperate in cross-border enforcement cases which transcend the enforcement capacities of any single PEA.[1281] APEC Economies wishing

---

can create significant privacy risks, for instance that information about the exercise of legal activities by persons in Canada could potentially be used against them, particularly where such activities are not legal or do not enjoy equal protection as in Canada ... How should the Government of Canada fulfill its responsibility to protect its citizens in these circumstances? One way may be to require organizations to seek meaningful consent when a transfer of personal information entails such risks. We would be interested to hear other effective solutions to this likely rare but significant problem for the exercise of rights. To be clear, we would not recommend that consent be required in the longer term in the context of data transfers for processing, if other effective means are found to protect the privacy rights of individuals. But in situations where neither contractual clauses nor other means are effective, consent may be required".

[1279] Office of the Privacy Commissioner of Canada, "Announcement: Commissioner Concludes Consultation on Transfers for Processing," last modified September 23, 2019, accessed December 24, 2019, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/.

[1280] The APEC is composed of the following Member Economies: United States; Australia; Brunei Darussalam; Canada; Chile; China; Hong Kong; Indonesia; Japan; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Philippines; Russia; Singapore; Republic of Korea; Chinese Taipei; Thailand; and Viet Nam.

[1281] The CPEA is the framework for regional cooperation among the privacy enforcement authorities established in the APEC region. It facilitates information sharing, cross-border investigation and enforcement. The list of the Privacy Enforcement Authorities participating to the framework is available at this link:

to join the system shall also identify the Accountability Agent that they intend to use: "[o]nce at least one Accountability Agent has been recognised in relation to that Economy, organisations will be able to commence participation in the CBPR system in the Economy".[1282] There are currently eight APEC Economies participating to the CBPR system: USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, and Chinese Taipei. For example, in the United States, the Federal trade Commission functions as the enforcement authority while TRUSTe is the accountability agent.[1283]

The CBPR system then requires companies in the Economy that has joined the system to meet the CBPR program requirements which set out the base level of protection that companies shall meet so as to be certified under the framework.[1284] In particular, companies are required to adopt internal privacy rules which shall be in line with the nine Privacy Principles set out under the APEC Privacy Framework endorsed in 2004 by the APEC Economies: 1) preventing harm; 2) notice; 3) collection limitations; 4) uses of personal information; 5) choice; 6) integrity of personal information; 7) security safeguards; 8) access and correction; 9) accountability.[1285] By making participation to the CBPR system dependent upon compliance with the APEC Privacy Framework, this requirement aims to "solve the problem of non – or variable – adoption of the Privacy Framework within the APEC region".[1286] This problem derives from the fact that, since APEC is a cooperative organization, the

---

https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

[1282] *APEC Cross-Border Privacy Rules System. Policies, Rules and Guidelines*, 2019, 8, accessed August 19, 2019, http://cbprs.org/documents/.

[1283] See TRUSTe website: https://www.trustarc.com/products/apec-certification/.

[1284] *APEC Cross-Border Privacy Rules System Program Requirements*, 2019, accessed August 31, 2019, http://cbprs.org/documents/. The CBPR program requirements were developed with the view of assisting Accountability Agents in verifying Applicants' compliance with the CBPR framework and with the view of ensuring that the compliance review process is carried out in a consistent manner throughout the APEC participating Economies.

[1285] *APEC Privacy Framework*, 2005, accessed August 31, 2019, https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework. Besides including nine data protection principles, the APEC Privacy Framework also comprises a guidance on the implementation of such principles both at the domestic level (for example by means of legislative, administrative, industry self-regulatory methods) and at the international level (for example by means of information sharing among Economies and international cooperation in cross-border cases). The framework was designed to ensure effective protection of personal data while maintaining data flow in the Asia Pacific region: "it balances information privacy with business needs and commercial interests, and at the same time, accords due recognition to cultural and other diversities that exist within member economies". Ibid., 3. The APEC Privacy Framework was updated in 2015: *APEC Privacy Framework*, 2015, accessed August 31, 2019, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

[1286] Andrei Gribakov, "Cross-Border Privacy Rules in Asia: An Overview," *Lawfare*, last modified January 3, 2019, accessed August 19, 2019, https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview.

Member Economies are not legally bound to implement the principles under the APEC Privacy Framework into their domestic legislation.[1287]

The internal rules developed by the applicant organizations will then need to be certified by the APEC-recognized Accountability Agents, which are hence responsible for reviewing companies' applications and for certifying their adherence to the CBPR requirements. Once such rules have been certified, they become *binding* and, consequently, *enforceable* against the companies in case of non-compliance.[1288] Accountability Agents are also responsible for monitoring and advising certified companies on compliance with the CBPR requirements; for solving disputes between certified organizations and individuals; and for enforcing CBPR requirements against the company in case of violation, for example, by removing the company from the CBPR system, by imposing penalties such as monetary penalties or compensation to the data subject. As it will analysed further below, in their enforcement actions, Accountability Agents complement and support the role of PEAs.[1289]

It should be stressed that the CBPR system delineated above is not legally binding on APEC participating Economies nor on the companies in those Economies. The system is, indeed, ultimately dependant on domestic legal components. This entails that conflicting domestic provisions may preclude Economies from joining the system, in which case it is up to the Economy concerned to make changes in order to make sure that the elements necessary for the functioning of the CBPR system are in place. This dependence on domestic legislation also entails that domestic provisions which prescribe a higher level of protection compared to the principles under the APEC Privacy Framework shall be complied with and hence maintained following transfer. On the other hand, where the requirements under the CBPR system provides for a level of protection which exceeds the level of protection prescribed under the domestic legislation, organizations will be able to join the system

[1287] *APEC Privacy Framework*, 30–33.

[1288] IBM was the first company certified under the CBPR system. "IBM Becomes First Company Certified Under APEC Cross Border Privacy Rules," *IBM*, last modified August 12, 2013, accessed August 19, 2019, www-03.ibm.com/press/us/en/pressrelease/41760.wss. The list of the companies that have been certified under the CBPR system is available at this link: http://cbprs.org/compliance-directory/cbpr-system/.

[1289] On the functioning of the CPBR system see *APEC Cross-Border Privacy Rules System. Policies, Rules and Guidelines*. See also, Information Integrity Solutions, *Towards a Truly Global Framework for Personal Information Transfers. Comparison and Assessment of EU BCR and APEC CBPR Systems*.

only if they voluntary comply with such additional requirements (although PEAs established in that country will still need to be able to take enforcement actions under the domestic law in compliance with the CBPR system).[1290]

The transfer of personal data from the CBPR-certified entity to a third party (whether domestic or international) is governed by principle 9 of the APEC Privacy Framework on "accountability". The said Principle provides that a "personal information controller should be accountable for complying with measures that give effect to" the Principles established under the APEC Privacy Framework. In particular, when a data controller transfers personal data "to another person or organization, whether domestically or internationally", the said controller should either obtain the consent of the individual concerned "or exercise due diligence and take *reasonable steps* to ensure that the recipient person or organization will protect the information consistently with" the Principles established under the APEC Privacy Framework.[1291]

Such "reasonable steps" may be taken by adopting internal guidelines or policies, implementing contracts, complying with applicable industry or sector laws and regulations, complying with self-regulatory applicant code or rules, and by implementing other agreements aimed at ensuring that transferred personal data continue to receive the same level of protection regardless of their location (question 46 of the CBPR program requirement). To this aim, such agreements shall generally require that the recipient abide by the data exporter's APEC-compliance privacy policies and practices, that it implements privacy practices substantially similar to the data exporter's privacy policies and practices, that it follows the data exporter's instructions on how data should be handled, and/or that it is CBPR-certified by an Accountability Agent in its jurisdiction (question 47 of the CBPR program requirement). Similarities with the model set out under PIPEDA emerge from these provisions. Indeed, like PIPEDA, in regulating the transfer of data to third parties, the APEC

[1290] *APEC Cross-Border Privacy Rules System. Policies, Rules and Guidelines*, 10–11. See also Information Integrity Solutions, *Towards a Truly Global Framework for Personal Information Transfers. Comparison and Assessment of EU BCR and APEC CBPR Systems*, 6.

[1291] Principle 9, APEC Privacy Framework (italics mine).

Framework does not focus exclusively on the jurisdiction to which the recipient is subject but it also recognizes that other tools, like contracts or internal policies or guidelines, could be implemented to ensure the required level of protection.[1292] The CBPR system is hence an example, like PIPEDA, of a data transfer regime based on an organization-to-organization approach since it holds organizations accountable for complying with the measures which give effect to the principles under the APEC Privacy Framework. At the same time, however, the CBPR system draws some elements from the geographical approach since "it encourages Member Economies to develop cooperative bilateral or multinational arrangements so that the participating countries will cooperate in the investigation and enforcement of data protection violations".[1293]

Once a company within a participating APEC Economy has certified under the framework, that certified company will be able to engage in "low friction" transfer of data to other CBPR-certified companies located in participating APEC Economies. Precisely, the CBPR system enables (1) data transfer from an entity acting as data controllers to another entity within the same corporate group but in different Economies (e.g., Google Australia transferring data about its users to Google Singapore) and (2) data transfer from an entity acting as data controllers to another company acting as data controller or as data processor in a different Economy and which is *not* part of the same corporate group. CBPRs are hence more flexible than BCRs since they allow companies (i.e., data controllers) to transfer data to data controllers and/or data processors outside their corporate group.[1294] At the same time, however, just like the corporate structure circumscribes the functioning and hence the potentials of BCRs, geography represents a limitation for the CBPR system. Indeed, CBPRs enable certified companies in participating APEC economies to engage in low friction transfers only to other APEC Economies which have joined the system. This entails that as soon as data are

[1292] Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 58.

[1293] Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 27.

[1294] Information Integrity Solutions, *Towards a Truly Global Framework for Personal Information Transfers. Comparison and Assessment of EU BCR and APEC CBPR Systems*, 7.

transferred to third parties in foreign destinations, "higher friction" solutions such as those listed in questions 46 and 47 of the CBPR program requirements will need to be implemented.[1295]

Moreover, like BCRs and EU data transfer provisions more broadly, CBPRs place great importance on the *enforcement* of data privacy rules. Indeed, as seen above, APEC Economies seeking to join the CBPR system must establish in their jurisdiction at least one PEA and one Accountability Agent which are responsible for enforcing the system, and the commitment to cooperate with such Authorities is an essential requirement for companies wishing to join (and stay in) the system. Moreover, and most importantly, *inter*-group transfers are made possible by the tight international cooperation between different PEAs in different Economies.[1296] Indeed, the EU-centric enforcement mechanism on which BCRs rely, and under which liability rests with the EU headquarter or with the EU BCR member with delegated responsibilities (even if the violation was caused by a non-EU BCR entity), is replaced under the CBPR system by a more distributed enforcement system. In other words, liability rests with the CBPR-certified company even if the violation was put in place by a third-party data controller or processor (in this case, however, the third party may be obligated to provide compensation to the CBPR-certified entity for any violations of the CBPR requirements). In the event that no resolution of the complaint can be reached within the jurisdiction of the CBPR-certified company that has transferred the data, the complaint can be taken before the enforcement authorities of the APEC Economy in which the CBPR-recipient is located:[1297]

[1295] Ibid., 32.
[1296] Ibid., 31–32.
[1297] Ibid., 10.

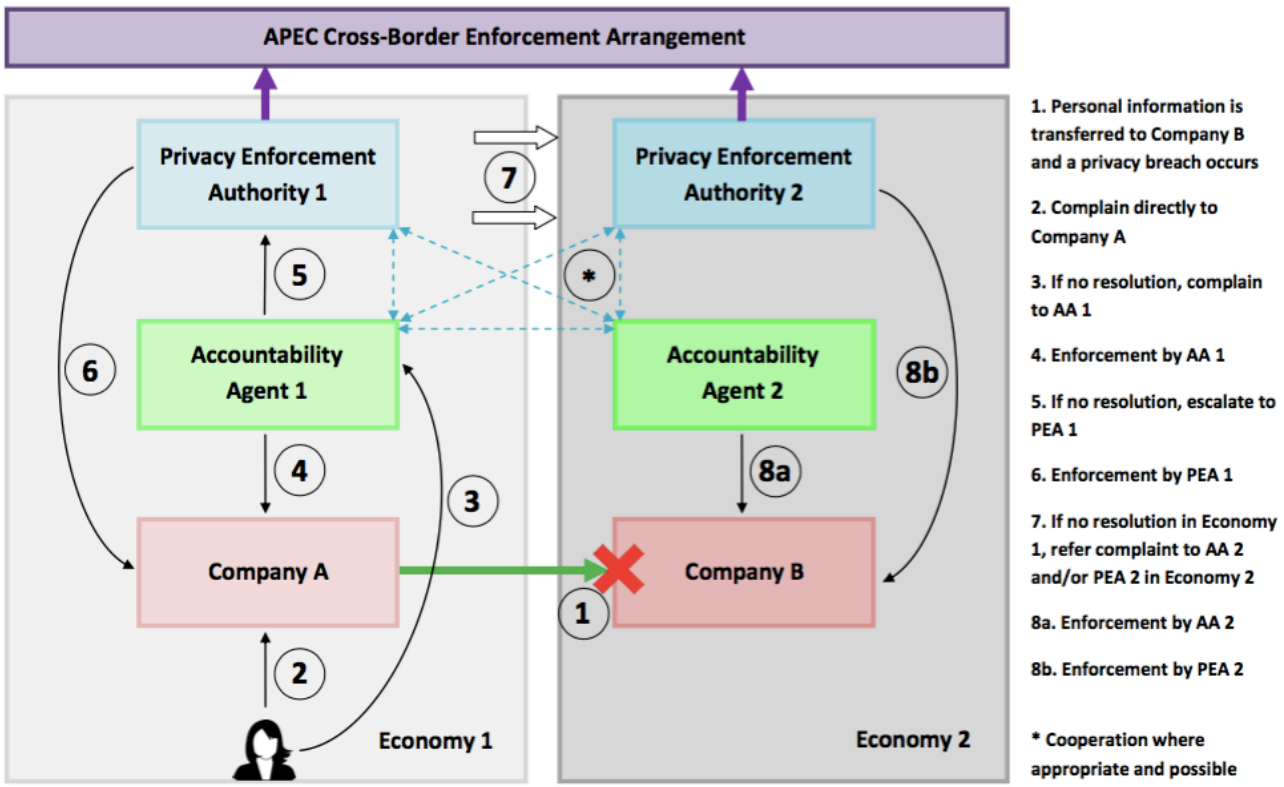

Figure 1- CBPR enforcement work-flow[1298]

The work-flow above makes clear that since data transfer may involve several CBPR-certified companies in several participating Economies, cross-border enforcement between enforcement authorities is essential, which is precisely the reason why the establishment of PEAs is a prerequisite for joining the system.[1299] In the light of the above, it can be concluded that the overarching principle underlying BCRs and CBPRs is essentially the same but its execution is different:

> the sending company should be accountable for the information that it transfers outside of the EU or APEC Economy and the individual complainant should be able to gain accessible redress for violation of the relevant privacy requirements. BCR achieves this by specifying one responsible EU entity. The CBPR System does so by fostering cooperation between Accountability Agents and PEAs in the APEC Economies where the transfer takes place.[1300]

The workflow above shows that the CBPR system is also designed so as to allow effective enforcement not only by the competent enforcement authorities but also by individuals. Indeed, under the APEC regime, individuals can complain to the Accountability Agents which is responsible for investigating complaints and solving disputes between the CBPR-certified company and individuals.

[1298] Ibid., 12.
[1299] Ibid., 35.
[1300] Ibid., 36.

As shown in the table, the possibility to escalate to PEAs is also included so as to address situations where the contested violation is not solved by the Accountability Agent. Individuals can also complain directly to the CBPR-certified company which, for this reason, shall have in place a procedure for receiving and investigating privacy-related complaints and remedial mechanisms to timely address such complaints.[1301]

The means that the CBPR system puts at data subjects' disposal for enforcing their rights hence differ from those available to individuals under BCRs. Indeed, under BCRs, data subjects can enforce organizations' privacy rules as third-party beneficiaries by either lodging a complain before the competent EU DPA or the competent court. However, these differences seem to be more *procedural* than substantive since both systems include redress mechanisms although through different avenues.[1302] A difference between the BCR and the CBPR systems is, however, the fact that, while under BCRs individuals are always entitled to seek a judicial remedy, under the CBPR system, whether data subjects have a private right of action depends on local data protection laws.[1303]

In 2015, the data transfer regime developed in the APEC region was further expanded with the development of the APEC Privacy Recognition for Processor (PRP) System, a recognition system which allows processors to be certified by an APEC-recognized Accountability Agent. The PRP was developed as a corollary of the CBPR which only applies to data controllers. This limited applicability of the CBPRs derives from the fact that the APEC Privacy Framework, on the basis of which CBPRs were designed, only lays out obligations for data controllers. The limited scope of CBPRs has led many data controllers to call for a system under which they could easily identify qualified data processor with whom to contract. Processors also expressed their interest in the development of a

[1301] Ibid., 15–16, 18 and 36. See also CBPR program requirement, questions 41, 42 and 43.

[1302] Ibid., 36; Malcolm Crompton, "East Meets West: Striving to Interoperable Frameworks?," *Data Protection Law & Policy* (May 2014): 13, accessed August 22, 2019, https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f62d08a65e232a6959d2b/1465869010281/IIS+Crompton+Shao+DPLP+May+2014+-+BCR+CBPR.pdf.

[1303] Article 29 Data Protection 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 (WP212)*, 2014, 17, accessed December 23, 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf.

system under which they could "signal" to data controllers their ability to provide effective implementation of controllers' privacy obligations. The PRP was hence designed to help processors that have been certified by Accountability Agents demonstrate their ability to process personal data consistently with the controller's privacy obligations set out under the CBPR System. This system is also meant to assist small and medium-sized companies to become "visible" to data controllers outside their economies and hence engage in international data processing relationships.[1304]

At the same time, it is important to stress that the PRP system does not alter the allocation of responsibility in the controller-processor relationship under the CBPR System:

> Under the Accountability principle in the Framework and the CBPR System, controllers are responsible for the activities processors perform on their behalf and they will remain so even when contracting with a PRP-recognized processor. Thus, processor activities remain subject to enforcement through enforcement against the controllers. This means that CBPR-certified controllers must apply due diligence in selecting their processors and engage in appropriate oversight over their processors, regardless of whether the processors are PRP recognized. Note that there is no requirement that a CBPR-certified controller must engage a PRP-recognized processor to perform information processing in order to comply with the Accountability principle in the Framework and the CBPR System.[1305]

In other words, in compliance with the principle of accountability, data controllers remain responsible for the data processing activities conducted by data processors on their behalf, even if the processors engaged by them have been certified by an Accountability Agent under the PRP system. This also entails that violations of the CBPR requirements from the data processors will lead to enforcement actions on the data controller who has outsourced the processing activities to that data processor. Several oversight and enforcement mechanisms are, however, in place to ensure data processors' compliance with the PRP program requirements.[1306]

Overall, and to sum up, the CBPR system consists of the initial verification of organizations' capacity to comply with the APEC Principles and on the subsequent oversight of ongoing compliance.

[1304] *APEC Privacy Recognition for Processors ("PRP"). Purpose and Background*, n.d., 1, accessed August 4, 2019, http://cbprs.org/documents/; *APEC Privacy Recognition for Processors System. Policies, Rules and Guidelines*, n.d., 2, accessed August 4, 2019, http://cbprs.org/documents/.

[1305] *APEC Privacy Recognition for Processors ("PRP"). Purpose and Background*, 1.

[1306] *APEC Privacy Recognition for Processors System. Policies, Rules and Guidelines*, 6; *APEC Privacy Recognition for Processors ("PRP"). Purpose and Background*, 2.

In this framework, the principle of accountability identifies both the actors which are *responsible* for ensuring compliance with the APEC Principles (and which should hence be *called to answer* in case of non-compliance) and the ability of such actors to *demonstrate* their capacity to comply with the Principles.[1307] As mentioned above, several similarities can be identified between BCRs and CBPRs since both systems are based on companies' commitments to process and secure data in compliance with the applicable data protection rules and on the certification by independent agents in the case of CBPRs and on the approval of the competent data protection authority in the case of BCRs (which is *de facto* a form of certification).[1308]

The ground is hence fertile for achieving interoperability between the two data transfer systems and, indeed, some steps have already been taken in this direction. Precisely, in 2012, the APEC Electronic-Commerce Steering Group's Data Privacy Subgroup set up a working group including representatives of the A29WP with the aim of exploring interoperability between EU data transfer mechanisms and the CBPR system. The discussions within the working group led to the adoption, in 2014, of a "Referential" in which the requirements for BCRs and the requirements for CBPRs are mapped and compared so as to provide companies seeking a double certification with a pragmatic checklist of the elements required under the two systems.[1309] Merck & Co. Inc., a multinational pharmaceutical company, became the first company to achieve approval for its BCRs on the basis of its CBPR certification. In other words, in a global first, Merck achieved dual certification by receiving first its CBPR certification in 2013 and subsequently, in 2016, approval

[1307] Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 58.

[1308] The CILP noted that, although certifications and BCRs "are presented as separate concepts, ... arguably, BCR are a de facto form of certification and it makes sense to elaborate the similarities between the two concepts. BCR-approved companies and their executive leadership all regard their BCR as a de facto certification of their privacy compliance program and a 'badge of recognition' by DPAs". Centre for Information Policy Leadership, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*, 2017, 12, accessed August 25, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

[1309] "This referential does not aim at achieving mutual recognition of both systems. However, it could serve as a basis for double certification. In any case, data protection policies of applicant international companies operating both in the EU and the APEC areas have to be approved respectively by the relevant bodies in the EU Member States and in the APEC Economies, in accordance with the applicable approval procedures". Article 29 Data Protection Working Party, *WP212*, 2.

from the EU regulators for its BCR application. In so doing, Merck achieved its BCR approval more rapidly and at lower costs compared to traditional BCR applications. After Merck, Box Inc. also obtained BCR approval after having certified under the CBPR, while Hewlett-Packard followed the reverse path: it certified under the CBPR after having obtained BCR approval.[1310]

Talks between the EU and the APEC on the steps that should be taken to achieve interoperability between the CBPR system and the EU data transfer mechanisms were renewed in 2017 when the APEC Electronic-Commerce Steering Group's Data Privacy Subgroup held a meeting with a representative of the European Commission in order to discuss a work plan on the facilitation of global data flow, especially in the light of the then-upcoming implementation of the GDPR.[1311] The European Commission also expressed its intention to harness "the full potential of the GDPR toolkit for international transfers"[1312] by working at the international level with organizations which have developed similar data transfer rules, such as the APEC. Ways to promote convergence between BCR and CBPRs could indeed be explored as regards both the applicable data protection standards and application process. According to the European Commission, this "should contribute to promoting high data protection standards globally while bridging differences in approaches to privacy and data protection, helping commercial operators to navigate between different systems and designing policies that comply with them".[1313]

[1310] Hilary Wandall and Daniel Cooper, "How to Align APEC and EU Cross-Border Transfer Rules," *LAW360*, April 12, 2016, accessed August 20, 2019, https://www.cov.com/-/media/files/corporate/publications/2016/04/how_to_align_apec_and_eu_cross_border_transfer_rules.pdf; "Merck Successfully Concludes First APEC-Based BCR Approval," *TrustArc Blog*, last modified March 22, 2016, accessed August 20, 2019, https://www.trustarc.com/blog/2016/03/22/merck-successfully-concludes-first-apec-based-bcr-approval/; Angelique Carson, "Merck First Company to Win BCRs via APEC's CBPRs," *Iapp*, March 22, 2016, accessed August 20, 2019, https://iapp.org/news/a/merck-first-company-to-win-bcrs-via-apecs-cbprs/; Daniel Cooper and Hilary Wandall, "Scaling Data Protection Globally through Interoperable Accountability," *Datenschutz und Datensicherheit - DuD* 41, no. 2 (February 1, 2017): 74–76.

[1311] "Data Privacy Subgroup Meeting with European Union," *Asia-Pacific Economic Cooperation*, accessed July 30, 2019, https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union.

[1312] European Commission, *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*, 10.

[1313] Ibid., 11.

6.4.2.5. The Accountability Principle in the EU Data Protection Framework

The principle of accountability is also embedded in the EU data protection framework. The most evident use of the accountability principle is represented by BCRs. Indeed, as seen above (5.5.2.), under BCRs continued protection to the transferred data is guaranteed by the implementation by a group of undertakings of internally and externally binding codes of conduct and by the acceptance of liability for any privacy breach by one entity (i.e., the EU headquarter or the EU BCR entity with delegated responsibility).[1314] Many obligations aimed at ensuring that the applicable data protection principles are put into effect shall, indeed, be included in BCRs. Among others, a data protection policy shall be in place; audit and training programs shall be set out; complaints shall be handled through an internal complaint mechanism; a record of the processing activities should be maintained; where required, a DPO shall be appointed or any other person responsible for monitoring compliance with the rules: "[i]n short, BCRs compel organisations to demonstrate how they are in compliance with all aspects of applicable data protection legislation".[1315]

Moreover, back in 2009, in their Joint response to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, the A29WP and the Working Party on Police and Justice suggested that the principle of accountability should be introduced in the EU data protection framework as a means to strengthen the responsibility of data controllers. Two obligations would stem from this principle: the obligation "to carry out the necessary measures to ensure that substantive principles and obligations of the current Directive are observed when processing personal data" and the obligation "to have the necessary internal

[1314] The Article 29 Working Party noted that "binding corporate rules ('BCRs'), which are used in the context of international data transfers, reflect the accountability principle. Indeed BCRs are codes of practice, which multinational organisations draw up and follow, containing internal measures designed to put data protection principles into effect (such as audit, training programmes, network of privacy officers, handling complaint system). Once reviewed by national data protection authorities, BCRs are deemed to ensure adequate safeguards for transfers or categories of transfers of personal data between companies that are part of the same corporate group and that are bound by these corporate rules ex Article 25 and 26.2 of Directive 95/46". Article 29 Data Protection Working Party, *Opinion 3/2010 on the Principle of Accountability (WP173)*, 2010, 7, accessed December 27, 2019, https://www.dataprotection.ro/servlet/ViewDocument?id=654. See also Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 106.

[1315] Organisation for Economic Cooperation and Development, *The OECD Privacy Framework*, 106. See also, criterion 6.1.2 for approval of BCRs, Article 29 Data Protection Working Party, *WP256 Rev.01*.

mechanisms in place to demonstrate compliance to external stakeholders, including national DPAs".[1316] The implementation of these obligations by data controllers would not only greatly strengthen the effectiveness of data protection rules but it would also facilitate competent DPAs in their supervision and enforcement tasks.[1317] At the same time, the A29WP and the Working Party on Police and Justice noted that the measures adopted by data controllers should be "scalable", meaning that the type of measures that DPAs should reasonably expect from data controllers should vary depending of several criteria, including the type and the size of the company, the amount and the nature of the processed data.[1318]

In commenting on the principle of accountability in relation to BCRs, the A29WP and the Working Party on Police and Justice even suggested that the EU data protection system could be innovated by including "from a general point of view, a new provision ... pursuant to which *data controllers would remain accountable and responsible for the protection of personal data* for which they are controllers, even in the case the data have been *transferred to other controllers outside the EU*".[1319] However, as noted by Moerel (2012), the inclusion of a similar provision would lead to an "accumulation" of requirements of two different data transfer regimes: (1) continued accountability and liability of the data exporters after transfer and (2) the existing EU legal bases for transfer and the related liability regime (e.g., joint and several liability under 2001 SCCs; acceptance of liability by one EU entity under BCRs).[1320] As stressed by Moerel, "[i]t is doubling requirements if companies with BCR have to comply both with the EU transfer rules (thus have to enter into the EU Standard Contractual Clauses with a third-party supplier) and on top of that be accountable for any data protection breach by such third party".[1321] Against this background, if the accumulation of these two different systems is not advisable, it could however be argued that the adoption of a similar provision

[1316] Article 29 Data Protection Working Party and Working Party on Police and Justice, *WP168*, 20.
[1317] Ibid., 3.
[1318] Ibid., 20.
[1319] Ibid., 12 (italics mine).
[1320] Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 224–225.
[1321] Ibid., 225.

on accountability would instead be acceptable if it is included *not on top of* existing data transfer mechanisms *but as an alternative to* them, along the lines of PIPEDA which, however, would lead to a complete overhaul of the existing EU data transfer regime.

One year later, in 2010, the A29WP further stressed the importance of the principle of accountability by issuing an entire opinion on the concept of accountability. In this opinion, the A29WP proposed to introduce the said principle in the revised 1995 Directive as a means to move data protection from theory to practice and hence as a means to ensure the effective implementation of the EU data protection rules. The A29WP firstly noted that, in general terms, the concept of accountability puts its emphasis "on showing how responsibility is exercised and making this verifiable".[1322] This is why, rather than focusing on the concept itself, the A29WP referred to the measures that should be put in place in order to ensure compliance with the applicable data protection rules and to make such compliance verifiable.[1323] In the opinion in question, the A29WP reiterated in greater detail the twofold obligations stemming from the principle of accountability which it had previously identified in WP168: the obligation to "to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with and to demonstrate so to supervisory authorities upon request".[1324] Accountability measures include the establishment of internal procedures before undertaking new data processing operations, data protection policies, the appointment of a data protection officer, training to staff members, the establishment of complaint handling mechanisms and of procedures for the management and the reporting of data breaches.[1325]

[1322] Article 29 Data Protection Working Party, *WP173*, 7.

[1323] "[w]e focus on the measures which should be taken or provided to ensure compliance in the data protection field. References to accountability should therefore be understood as the meaning used in this Opinion, without prejudice to finding another wording that more accurately reflects the concept given here. This is why the document doesn't focus on terms but pragmatically focuses on the measures that need to be taken rather than on the concept itself". Ibid., 8.

[1324] Ibid., 2. The A29WP even proposed a possible wording for a provision on the principle of accountability: "*Article X - Implementation of data protection principles. 1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with. 2 The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request"* (Ibid., 10.).

[1325] Article 29 Data Protection Working Party, *WP173*, 11–12.

Two clarifications are necessary in order to understand how the principle of "accountability" works in practical terms. Firstly, as stressed by the A29WP, the implementation of the accountability principle does not entail a change in the substantive data protection rules that apply to the data processing but it aims to make such rules more effective.[1326] Secondly, fulfilling the accountability principle does not necessarily entails that the controller is compliant with the substantive data protection principles nor is there a presumption of such compliance: a "data controller may have implemented and verified the measures that it has put in place; and yet it may find itself engaged in wrongdoing". In other words, adopting measures to implement and demonstrate compliance with the relevant data protection principles does not exempt the data controller from enforcement actions in the event of violations. Rather, the practical result of having implemented such measures is, on the one hand, that the data controller is less likely to be in breach of the law and, on the other hand, that, in the event of violation, the data protection authorities "could give weight to the implementation (or lack of it) of measures and their verification" in assessing sanctions.[1327]

The principle of accountability is now explicitly integrated in the GDPR. Article 5(2) GDPR indeed provides that the "controller shall be responsible for, and be able to demonstrate compliance with" the principles relating to the processing of personal data listed under Article 5(1) GDPR: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality.[1328] The principle of accountability hence makes it clear that the data controller is *responsible* for ensuring compliance with data protection principles and that data controller shall be able to *demonstrate* such compliance. Being able to *demonstrate* that appropriate measures have been implemented by the organization is particularly relevant in case a privacy breach occurs since it may favour a more lenient approach by the competent data protection

[1326] Ibid., 5.
[1327] Ibid., 11.
[1328] Article 5 GDPR. See also Article 24(1) GDPR under which "[t]aking 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 organisational 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".

authorities in their enforcement actions. At the same time, it should be stressed that, under the GDPR, the principle of accountability does not only apply to controllers but also processors are expected to comply with certain accountability obligations. Among others, processors shall "implement appropriate technical and organisational measures"[1329] to meet the requirements under the GDPR; they shall maintain records of processing;[1330] cooperate with DPAs,[1331] and appoint a data protection officer.[1332] This reflect the fact that data protection is a shared responsibility between controllers and processors.[1333]

Organizations are hence required to adopt a *proactive* approach to data protection, meaning that they are required not only to put in place appropriate organizational and technical measures but also to keep evidence of all the steps they have taken to protect people's privacy. Such measures shall also be kept under review and updated when appropriate. The implementation of a privacy management framework is particularly welcomed especially for larger organizations since it would help embed compliance within the organization and "create a culture of privacy".[1334] In this regard, Article 24(2) GDPR explicitly provides that, "[w]here proportionate in relation to processing activities", the organisational and technical measures adopted by data controllers "shall include the implementation of appropriate data protection policies".[1335]

Accountability is hence fully integrated among the EU basic data protection principles. This is also witnessed by the fact that, in updating in 2017 (WP254) its 1998 guidelines on transfers of personal data to third countries (WP12), the Article 29 Working Party has included the principle of

---

[1329] Article 28(1) GDPR.

[1330] Article 30 GDPR.

[1331] Article 31 GDPR.

[1332] Articles 37-39 GDPR.

[1333] On the accountability obligations and other legislative obligations that the GDPR imposes on processors, see Centre for Information Policy Leadership, *The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society*, 2018, 11–12 and 15–18, accessed August 25, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

[1334] Information Commissioner's Office, "Accountability and Governance," accessed December 27, 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.

[1335] Article 24(2) GDPR. On the principle of accountability, see also Lindqvist, "New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?," 57–59.

accountability among the basic procedural/enforcement data protection principles that a third country's legal order shall contain in order to be found adequate. In particular, under the said principle

> A third country data protection framework should oblige data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority. Such measures may include for example data protection impact assessments, the keeping of records or log files of data processing activities for an appropriate period of time, the designation of a data protection officer or data protection by design and by default.[1336]

The European Commission's decision on the adequacy of the level of protection offered by Japan, indeed, includes the Commission's finding on the implementation of the principle of accountability within the Japanese data protection framework.[1337] Overall, the inclusion of accountability among the principles against which the adequacy of third countries is assessed should be welcomed as a means to ensure that the "adequate" level of data protection provided by the third country's legal order is effectively complied with by data recipients.[1338]

6.4.2.6. The Potentials and the Benefits of the Accountability Principle according to the Centre for Information Policy Leadership

The potentials of the accountability principle in the data protection field have also been explored by the Centre for Information Policy Leadership which from 2009 to 2013 conducted a project on accountability-based privacy governance. The first phase of the accountability project (the Galway Project) defined the essential elements of accountability as a result of a process which involved experts from the government, academia and the industry and which was facilitated by the Irish Data Protection Authority. The accountability principle, as understood and elaborated by the

[1336] Article 29 Data Protection Working Party, *Adequacy Referential (Updated) (WP254)*, 8.

[1337] Recitals 70-74, EU-Japan Adequacy Decision.

[1338] Even before the release of WP154 by the A29WP, several authors had suggested that the principle of accountability should be integrated in existing data transfer mechanisms in order to boost their effectiveness. Bennett (2010), for example, stressed that accountability instruments should not be seen as alternatives to adequacy assessments but rather as "ways to make the adequacy framework work more effectively". Bennett, "International Privacy Standards: Can Accountability Be Adequate?," 23. Along the same lines, Alhadeff et al. noted that "the applicability of legislation offering 'adequate' safeguards does not by itself ensure that appropriate guarantees are implemented in practice". This is why "[r]equiring the demonstration of the recipient's capacity to comply, in addition to the requirement of adequacy, could provide additional assurance that adequate protection mechanisms will effectively be in place". Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 69.

CILP, requires companies not only to be *responsible* for the data they handle but also to *demonstrate* their willingness and their capacity to protect personal data in accordance with the applicable data protection rules. The CILP mainly focused on the principle of accountability as an instrument of *global data governance* which requires companies to set privacy protection goals, to determine the measures to achieve those goals and to demonstrate their capacity to comply with the applicable data protection rules: accountability "involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practices, and vesting the organisation with both the ability and the responsibility to determine appropriate, effective measures to reach those goals".[1339]

The essential elements of an accountability-based approach to data governance identified by the CILP are the following:

> 1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria.
> 2. Mechanisms to put privacy policies into effect, including tools, training and education.
> 3. Systems for internal, ongoing oversight and assurance reviews and external verification.
> 4. Transparency and mechanisms for individual participation.
> 5. Means for remediation and external enforcement.[1340]

An accountability-based approach to data governance hence requires companies to set data protection goals which are consistent with the external legislation (essential element 1) and to establish the measures to achieve those goals, including personnel training and education (essential element 2); accountable organizations should verify on an ongoing basis the effectiveness of their measures in protecting and securing data by means of internal and external oversight (essential element 3); organisations' practices should be transparent and understandable to individuals (essential element 4); lastly, organizations should include in their privacy policy mechanisms to handle and address

[1339] Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 2009, 2–3, accessed August 5, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_protection_accountability-the_essential_elements__discussion_document_october_2009_.pdf.

[1340] Ibid., 4.

individuals' complaints and should recognize and respond to enforcement actions by competent authorities (essential element 5).[1341]

Most importantly, the CILP stressed the potentials of the principle of accountability as a means to bridge different regulatory approaches to data protection and hence as a vehicle to ease movement of data between organizations in different jurisdictions. Accountability, as an instrument of global governance, indeed, provides for continued protection to the data wherever it is processed as it "relies less on the rules that exist *where* the data is *processed* and more *where* the *obligation* is *first established*".[1342] At the same time, however, besides stressing that "[a]ccountability requires an organisation to remain accountable no matter where the information is processed",[1343] a detailed description of the practical functioning of a data transfer regime based on the accountability principle was not provided (at least not in this phase of the project).[1344]

In the second phase of the accountability project, the so-called Paris project, the CILP further detailed the "Common Fundamentals of an Accountability Implementation Program", and hence the common fundamentals that accountable organizations[1345] should be able to demonstrate to enforcement authorities and that such authorities should measure: 1) policies;[1346] 2) executive oversight;[1347] 3) staffing and delegation;[1348] 4) education and awareness;[1349] 5) ongoing risk

[1341] Ibid., 11–14.
[1342] Ibid., 9-10 (italics mine).
[1343] Ibid., 9.
[1344] See the analysis conducted further below on "global binding corporate rules" proposed by the CILP.
[1345] In the Paris project, accountability is described as follows: "a demonstrable acknowledgement and assumption of responsibility for having in place appropriate policies and procedures, and promotion of good practices that include correction and remediation for failures and misconduct. It is a concept that has governance and ethical dimensions. It envisages an infrastructure that fosters responsible decision-making, engenders answerability, enhances transparency and considers liability. It encompasses expectations that organisations will report, explain and be answerable for the consequences of decisions about the protection of data. Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data". Centre for Information Policy Leadership, *Demonstrating and Measuring Accountability. A Discussion Document*, 2010, 2, accessed August 9, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/demonstrating_and_measuring_accountability_a_discussion_document__accountability_phase_ii-the_paris_project_october_2010_.pdf.
[1346] "Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards". Ibid., 6.
[1347] "Internal executive oversight and responsibility for data privacy and protection". Ibid.
[1348] "Allocation of resources to ensure that the organisation's privacy program is appropriately staffed by adequately trained personnel". Ibid.
[1349] "Existence of up-to-date education and awareness programs to keep employees and on-site contractors aware of data protection obligations". Ibid.

assessment and mitigation;[1350] 6) program risk assessment oversight and validation;[1351] 7) event management and complaint handling;[1352] 8) internal enforcement;[1353] 9) redress.[1354] As stressed by the CILP, these fundamentals are only meant to provide guidance to accountable organizations. Indeed, "[a]ccountability is not a 'one-size-fits-all' approach". Rather, organisations should establish what measures are appropriate for their business on a case-by case basis: "all organisations will need to determine, consistent with recognized external criteria, which of these nine and/or others they will implement. The fundamentals should be applied in a way that is appropriate to the organisation's business model, data holdings, technologies and applications, and the risks to privacy they raise for individuals".[1355]

In 2011,[1356] in its response to the European Commission's Communication on a comprehensive approach to personal data protection, CILP suggested that the EU data protection framework could be innovated by building a new data transfer regime explicitly based on accountability: "Binding Global Codes". In particular, CILP suggested that, by way of derogation from Article 25 DPD (now Article 45 GDPR) under which data can only be transferred to third countries which ensure an adequate level of protection, organizations (data controllers) should be able to transfer data on the basis of a Binding Global Code adopted by the said organization and when data continue to be processed in accordance with that code after transfer. Companies should hence be allowed to develop and implement their own set of legally binding rules for ensuring and

[1350] "Implementation of a process to assist the organisation in understanding the risks to privacy raised by new products, services, technologies and business models, and to mitigate those risks". Ibid.

[1351] "Periodic review of the totality of the accountability program to determine whether modification is necessary". Ibid., 7.

[1352] "Procedures for responding to inquiries, complaints and data protection breaches". Ibid.

[1353] "Internal enforcement of the organisation's policies and discipline for non-compliance". Ibid.

[1354] "The method by which an organisation provides remedies for those whose privacy has been put at risk". Ibid.

[1355] Ibid., 4.

[1356] In 2011, the third phase of the accountability project was convened by the CILP. This is called the Madrid Project since discussions were facilitated by the Spanish DPA. The Project analysed the implementation of accountability in the marketplace, the measures that accountable organizations should implement, and the benefits that would accrue to the marketplace, data subjects, regulators and organizations from a widespread implementation of accountability requirements. Centre for Information Policy Leadership, *Implementing Accountability in the Marketplace A Discussion Document*, 2011, accessed August 25, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/implementing_accountability_in_the_marketplace__accounrtability_phase_iii-the_madrid_project_november_2011_.pdf.

demonstrating continued compliance with the EU data protection rules regardless of data location.[1357] Precisely,

> A "Binding Global Code" means a set of *legally binding* rules which require *contractually or otherwise*, that *regardless of location*:
> a. the personal data will be processed in accordance with the principles and obligations set out in the [Data Protection] Directive; and
> b. adequate safeguards will be observed with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.[1358]

The organization should apply such rules globally to all the processing carried out by it and it should *extend by contract* or otherwise the application of such rules to other organisations with which it shares the data. Moreover, as stressed by CILP, such rules should be "legally binding" , meaning "that the controller is liable, whether to a supervisory authority or to any adversely affected data subject, for any non-compliance with" the rules.[1359] In other words, data protection authorities should have the authority to investigate and impose sanctions in case of non-compliance with the commitments under the code and individuals should be able to enforce the code against the organisation when non-compliance with the code has caused harm to them.

However promising this system may sound, the exact functioning of the proposed Binding Global Codes is unclear and the fact that the EU data exporter which has adopted the code is required to contractually or otherwise extend the application of its internal rules to other non-EU organizations may, *de facto*, translate into the implementation of SCCs or other contractual solutions provided under the existing EU data transfer regime. The liability regime also seems unclear. Indeed, the CILP

[1357] The CILP suggested that companies should be allowed to self-certify their own code without going through the approval by a data protection authority in order to avoid bureaucratic deadlocks which have so far hampered the smooth functioning of BCRs. As a less radical alternative to self-certification, the CILP proposed that companies should have their Binding Global Code certified by independent third parties, which remind of the accountability agents under the CBPR framework. Centre for Information Policy Leadership, "A New Approach to International Transfers in Response to the European Commission's Communication on 'A Comprehensive Approach to Personal Data Protection,'" in *Accountability: A Compendium for Stakeholders*, 2011, 7, accessed August 10, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders__march_2011_.pdf.

[1358] Ibid., 9 (italics mine).

[1359] "'Legally binding' means that: a. the rules are legally enforceable and binding in practice so that the controller is liable, whether to a supervisory authority or to any adversely affected data subject, for any non-compliance with them; and b. the controller is committed to demonstrate to a supervisory authority on request how compliance is and will be achieved". Ibid., 9.

stressed that, under the proposed framework, organisations would need to accept responsibility for the fulfilment of the terms of the code and should hence be held accountable vis-à-vis individuals and enforcement authorities.[1360] However, it is unclear whether such liability would "stick" with the exporting organization even in the event that the privacy breach is attributed to the non-EU data importer.

6.4.3. The Way Forward

The analysis conducted above shows that the primary role of the principle of accountability is not only to identify the entity responsible for compliance with the applicable data protection rules but also to ensure that the said entity implements the necessary measures for *ensuring* compliance with the applicable data protection rules and for *demonstrating* such compliance. It is also clear that the principle of accountability does not alter the substance of the applicable data protection rules. Rather, it is designed to make the implementation of such rules more effective. The analysis conducted above has also shown that, in some cases, the principle of accountability has been developed as a vehicle for cross-border data flow, such as in the case of PIPEDA, CBPRs and BCRs. Indeed, all these data transfer mechanisms have embodied an organization-to-organization approach which, instead of restricting data transfers to other jurisdictions, allows organizations to develop internal organizational measures as a means to safeguard data regardless of their location. Moreover, the criteria for approval of BCRs and the criteria for participating in CBPRs share many similarities since, in both cases, the assessment of companies' capacity to comply with the applicable data protection rules is the determinative element for their inclusion in the system.[1361]

Calls for an accountability-based data transfer regime have been voiced by many parties, both in academia and in the private sector, as a means to overcome many of the limitations which affect the EU data transfer regime. Bird & Bird LLP for example, in its response to the Consultation on the

[1360] Ibid., 6–8.

[1361] Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 68–69.

legal framework for the fundamental right to protection of personal data launched by the European Commission in 2009, noted that "[t]he current system for regulating the transfers of data to countries outside the EU is no longer fit-for-purpose". Bird & Bird hence recommended the establishment of an accountability model as a development of the approach adopted under BCRs in which the exporting organisation remains responsible for the lawful processing of the data after transfer: "[t]his would push the burden of ensuring compliance onto the exporting organisation, and away from the regulator". This system would also be beneficial for data subjects which, in case of non-compliance, could seek remedies against the data exporter in the EU rather than against the non-EU importer.[1362] Interestingly, a somewhat punitive approach was put forward by Linklaters in response to the same consultation. Indeed, Linklaters suggested that the data exporter should remain liable for all the subsequent processing of the transferred data *unless* the transfer is framed under one of the legal bases for transfer laid out under the 1995 Directive (now GDPR). Continuing liability for any subsequent processing was hence proposed by Linklaters as a form of incentive for data exporters for complying with data transfer rules. Data exporter would so have the choice of either complying with data transfer rules or being liable for the subsequent processing of the transferred data. As a result, "[d]ata exporters who have previously ignored the rules on transborder dataflow would now have a strong incentive to comply".[1363]

Along the same lines, Microsoft responded to the same consultation by stressing the need to reform international data transfer mechanism "to cope with the growing volume and complexity of cross-border data movements".[1364] In particular, according to Microsoft Corporation, "[e]nsuring continued strong protection for EU-origin personal data, regardless of location, should continue to be the objective of EU rules on international transfers".[1365] The principle of accountability may help

[1362] Bird & Bird LLP, *Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009, paragraphs 11-12.

[1363] Linklaters, *A Framework Fit for the Twenty-First Century. A Response to the Commission's Public Consultation*, 2009, x, accessed August 12, 2019, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/unregistered_organisations/linklaters_llp_en.pdf.

[1364] Microsoft Corporation, *Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2.

[1365] Ibid., 7.

ensure such continued protection by holding data controllers accountable for compliance with EU data protection legislation regardless of location.[1366] Similarly, Intel Corporation stressed that "[s]o long as an organisation of any size provides adequate protection and accountability, transfers of personal data should take place without need for complex, lengthy and costly administrative processes".[1367] Along the same lines, Digital Europe suggested that "[r]egardless of the country in which the information is processed or stored the transfer of information should not be prohibited, provided that the company complies with and remains accountable to the applicable legal requirements".[1368]

In the light of the above, there seems to be a widespread agreement about the importance of the role that the principle of accountability may play in facilitating data transfer while guaranteeing continued protection to the transferred data. At the same time, however, little practical guidance has been provided about what an accountability-based data transfer regime compatible with the existing EU data protection framework should look like. Kuner (2009), for example, suggested that the principle of accountability could be explored as a means to overcome the proven "inadequacy" of adequacy decisions in protecting data effectively. According to Kuner, the principle of accountability would enable the establishment of a more flexible data transfer framework since, instead of relying on the lengthy process which normally precedes the adoption of adequacy decisions, it relies on the precautions taken on a case-by-case basis by the data exporters. At the same time, however, Kuner did not get into the details of how a data transfer regime based on accountability would work in practice within the EU framework.[1369] In order to get into these practical details, the following

[1366] Ibid., 8-9.

[1367] Intel Corporation, *Response to European Commission Public Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009, 4, accessed August 12, 2019, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/intel_corporation_en.pdf.

[1368] Digital Europe, *Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009, 6, accessed August 12, 2019, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/digital_europe_en.pdf.

[1369] As a first step, Kuner suggests that "it would be necessary to investigate what legal mechanisms could ensure that data exporter remained accountable and responsible for data processing once such data have been transferred outside the EU. This might include reliance on liability concepts under national law, or use of data transfer mechanisms that are

question should be addressed: which of the two main accountability-based data transfer regimes that have been developed in foreign jurisdictions (i.e., PIPEDA and CBPRs) include the most promising elements that, if integrated in the EU data protection framework, could significantly boost the EU data transfer regime and international data transfer more broadly?

PIPEDA is often mentioned as a good example of how the accountability principle could boost international data transfer while safeguarding data regardless of their location. However, as seen above (6.4.2.3.), the OPC itself has recently questioned the effectiveness of the principle of accountability in protecting data and suggested that the system of *de facto* self-regulation should be replaced by a proactive intervention by an independent regulator in reviewing the measures implemented by data controllers, which could even lead to the adoption of SCCs-like contractual clauses. Several criticisms have also been put forward against CBPRs which, from an EU perspective, do not seem to offer appropriate safeguards as a data transfer tool.[1370] This is clearly witnessed by the fact that Supplementary Rule 4 of the EU-Japan adequacy decision excludes onward transfer on the basis of the CBPR system to which Japan is a participating Economy. This was motivated by the fact that "in that system the protections do not result from an arrangement binding the exporter and the importer in the context of their bilateral relationship and are clearly of a lower level than the one guaranteed by the combination of" the Japanese Act on Protection of Personal Information and the Supplementary Rules.[1371] In this regard, the European Commission noted that, for example, "no

already recognized, such as binding corporate rules or the use of standard contractual clauses". Christopher Kuner, "Developing an Adequate Legal Framework for International Data Transfers" (2009): 8, accessed August 21, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1464323.

[1370] The APEC framework and the CBPR system has been severely criticized, among others, by Greenleaf. See Graham Greenleaf, "Five Years of the APEC Privacy Framework: Failure or Promise?," *Computer Law & Security Review* 25, no. 1 (2009): 28–43; Graham Greenleaf, *APEC's Cross-Border Privacy Rules System: A House of Cards?* (UNSW Law Research Paper No. 2014-42, 2014), accessed August 22, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468782; Graham Greenleaf, *Accountability Without Liability: 'To Whom' and 'With What Consequences'? (Questions for the 2019 OECD Privacy Guidelines Review)* (UNSW Law Research Paper No. 19-67, 2019), accessed August 22, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384427. See also Nigel Waters, *The APEC Asia-Pacific Privacy Initiative: A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation?* (UNSW Law Research Paper No. 2008-59, 2008), accessed August 22, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1402445.

[1371] Recital 79, EU-Japan adequacy decision. The EDPB also "welcomes the efforts made by the Japanese authorities and the European Commission to enhance the level of protection for onward transfers in Supplementary Rule (4), which excludes that personal data transferred from the EU is further transferred to a third country on the basis of

definition and specific protections for sensitive data, no obligation of limited data retention" are included in the CBPR system.[1372]

Certainly, similarities as well substantial differences emerge when conducting a side-by-side comparison between the principles under the EU data protection framework and the nine principles under the APEC Privacy Framework. The EU has, indeed, adopted stronger and more detailed principles compared to the APEC region which reflect the stronger geopolitical cohesion within the EU region and its approach to privacy as a fundamental human right. On the other hand, the Principles set out under the APEC Privacy Framework have been drafted so as to accommodate the different cultural and political systems of the 21 APEC Economies and, from an EU perspective, its prominent focus on trade objectives seems to unduly compromise individuals' privacy. Moreover, unlike the GDPR, the APEC Privacy Framework does not aim to establish a comprehensive data protection framework by which APEC Economies should be bound but it aims to set out some basic data protection standards that the APEC Economies *agree* to implement.[1373]

APEC- CBPRs". European Data Protection Board, *Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan*, 18.

[1372] EU-Japan adequacy decision, 14n50. For a critical analysis of Supplementary Rule 4 which has closed the "Japanese back-door" of onward transfer based on the CBPR system, see Graham Greenleaf, *Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles* (UNSW Law Research Paper No. 18-53, 2018), 10–13, accessed August 22, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3219728.

[1373] Information Integrity Solutions, *Towards a Truly Global Framework for Personal Information Transfers. Comparison and Assessment of EU BCR and APEC CBPR Systems*, 32–33; Sullivan, "EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era," 4–5 and 10–11.

For an analysis of the commonalities and the differences between the GDPR provisions and the APEC Privacy Framework, see also María Vasquez Callo-Müller, *GDPR and CBPR: Reconciling Personal Data Protection and Trade* (APEC Policy Support Unit - Policy Brief No. 23, 2018), 7, accessed August 19, 2019, https://www.apec.org/Publications/2018/10/GDPR-and-CBPR---Reconciling-Personal-Data-Protection-and-Trade; Gribakov, "Cross-Border Privacy Rules in Asia: An Overview."

Moreover, the CBPR has so far attracted little attention from both Economies and companies. Indeed, since its inception in 2011, only 29 companies have certified under the system. Cromption (2014) traces this "underperformance" back to the "chicken-and-egg problem". Indeed, according to Cromption, "Economies are slow to move without industry pressure for them to participate, while private sector organisations do not see a pressing need to join when the system is comprised of few Economies. Going forward, sustained efforts are required on the part of CBPR policymakers to highlight the benefits, as well as to offer incentives, for participation. As with any network effect, once more players come on board, the value and appeal of the system will increase accordingly". Cromption, "East Meets West: Striving to Interoperable Frameworks?," 12. On the need to achieve "critical mass" in order to realize the numerous potentials of the CBPR system, see also Markus Heyder, "The APEC Cross-Border Privacy Rules—Now That We've Built It, Will They Come?," *Iapp*, September 4, 2014, accessed August 23, 2019, https://iapp.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come/.

At the same time, the CBPR system seems to be built on some promising components for boosting international data transfer. Indeed, CBPRs should not be seen as a system to be transplanted and implemented as it is in the EU framework but rather as a *procedural scheme* for regulating international data transfer which could be filled with different *substantive rules* and integrated within the EU data protection realm. In particular, it appears that the CBPR system includes, and shares with the BCR system, several features which seems to be suitable for framing a smooth, efficient, scalable – meaning that it could potentially be expanded to any region and organization – international data transfer: (1) a *baseline level of data protection* which takes the form of *internal policies* adopted by companies and which is demonstrated through (2) *initial certification* and *ongoing audit* and which is (3) enforced by *data protection authorities* and (4) via *redress mechanisms* by data subjects.[1374]

These elements, which characterize both the CBPR system and the BCRs, should hence be regarded as building blocks on which a "new" (although built on existing elements) data transfer regime should be built. In more detail, such regime should be based on accountability as a way to address the limitations of existing legal bases for transfer by placing on companies most of the responsibility for ensuring compliance with external legislation through their internal privacy management programs (element 1). Companies should also demonstrate such compliance through initial certification and ongoing oversight (element 2). This form of "meta-regulation" (i.e., "the regulation of internal self-regulation")[1375] should then be backed up by public enforcement and by the implementation of redress mechanisms for data subjects (elements 3 and 4). Under the proposed system, accountability is hence understood as the obligation for companies to take their responsibility seriously by putting in place the necessary measures to comply with the applicable data protection

[1374] Cromption, "East Meets West: Striving to Interoperable Frameworks?," 12.

[1375] Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 178. The term "meta-regulation" is used to identify the regulatory initiatives that aim to encourage companies to build responsibility into their internal structure, practices and corporate culture. One of the main drivers for meta-regulation is "the recognition in the general policy literature that prescriptive regulation (where regulators prescribe the desired behaviour) has 'inherent limitations to achieve the underlying regulatory objectives due to "regulators" imperfect access to factual information and to theoretical knowledge (eg of the solutions that could most effectively and efficiently mitigate risks to regulatory objectives). More fundamental, prescriptive regulation is an inherently limited tool for managing complex, heterogeneous, and dynamic social realities, which leads to both excessive and insufficient regulation'". Ibid., 179.

rules and to demonstrate compliance to external stakeholders, i.e., DPAs and data subjects. This system should hence be based on a "narrow" definition of accountability which mainly focuses on the *measures* which should be implemented to make compliance effective and verifiable (and hence as an instrument of data governance as understood by CILP), rather than on accountability as "having primary responsibility and liability for data regardless of location",[1376] as it is the case under PIPEDA and the CBPRs.

Let's now analyse the first proposed building block for an accountability-based data transfer regime: a *baseline level of data protection* which takes the form of *internal policies* adopted by companies. Building on the successful experience of BCRs and on the promising experience of CBPRs, effective compliance with the EU basic data protection rules should be provided by companies' internal measures and policies, and hence by their privacy management program. In line with the certification mechanism under Article 42(2) GDPR, and in line with CBPRs, such internal policies should be adopted by the non-EU data importer wishing to receive data from the EU and not by the exporter organization. This would allow non-EU data importers to signal to EU companies their "reliability" and EU data exporters to easily identify non-EU data importers which are able to process data in compliance with the EU data protection standards. Moreover, the fact that appropriate safeguards are provided by the non-EU data importer rather than by the EU data exporter would allow the data exporter to "smoothly" transfer data to the "whitelisted" non-EU importer without worrying about contractually, or otherwise, expanding adequate protection to the non-EU data importer.[1377]

The accountability requirements to be found in privacy management programs should not only include internal rules mirroring external legislative criteria but also organizational arrangements

[1376] W. Kuan Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens* (Cheltenham, UK: Edward Elgar Publishing, 2017), 13, 38–39.

[1377] Along the same lines, in commenting on the Binding Global Code proposed by the CILP, Moerel noted that it would not be necessary for the exporting organization to contractually impose on its external supplier the terms of its code if the external supplier has implemented its own Binding Global Code. A similar solution would, indeed, be preferable since non-EU suppliers may struggle to implement BGCs from each of the EU companies on whose behalf they process personal data: "[w]hat is relevant is that the data obtain an adequate level of protection, not that the original Binding Global Code remains applicable to all other parties subsequently processing that data in the chain". Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 214.

designed to put such policies into effect, including training programs, audits, complaint handling systems, and the commitment to cooperate with the competent data protection authorities. In particular, these accountability requirements may mirror the essential elements and the "common fundamentals of an accountability implementation program" identified by the CILP. As seen above, such elements include not only the establishment by organizations of "binding and enforceable written" privacy policies[1378] consistent with external legislation, but also of *means for remediation* to individuals who have suffered harm and *external enforcement* by local regulators.[1379]

The reason why the common fundamentals identified by the CILP seems to offer useful guidance on how accountability requirements should be shaped derives from the fact that such requirements are set as general obligations. This would enable a customized approach to accountability under which companies could determine the elements of their privacy management programs on the basis of their business model, data holding and, more broadly, on the basis of the risks that their data processing poses to individuals.[1380] The said customized approach to accountability would also allow SMEs, which are often subject to resource-constraints, to tailor the accountability requirements to their specific needs.[1381] In the light of this, accountability requirements should be worded so as to focus more on the *outcomes* that companies should achieve rather than on the *means* for achieving such outcomes. This would also provide organizations with the necessary flexibility to adopt and adapt their privacy management programs on the basis of the constantly evolving challenges to data protection:[1382] "descriptions of the means by which multinationals should achieve data protection compliance are outdated the moment they are issued and stifle innovation as

[1378] Centre for Information Policy Leadership, *Demonstrating and Measuring Accountability. A Discussion Document*, 6.

[1379] Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 11–14; Centre for Information Policy Leadership, *Demonstrating and Measuring Accountability. A Discussion Document*, 6–7.

[1380] Centre for Information Policy Leadership, *Demonstrating and Measuring Accountability. A Discussion Document*, 4.

[1381] Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 17; Centre for Information Policy Leadership, *The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society*, 22.

[1382] Centre for Information Policy Leadership, *The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society*, 19.

regards the most effective means to achieve data protection compliance in practice".[1383] In the light of the above, Moerel even suggested that the main criteria for approval of BCRs should (have) be(en) designed on the basis of the CILP's common fundamentals of accountability.[1384]

Let's now move to the second element of the proposed system: *initial certification* and *ongoing audit*. This element is consistent with the fact that, under both BCRs and CBPRs, companies are admitted to the "club" if their privacy rules have been approved by the competent DPA under the BCR system, and by Accountability Agents under CBPRs. This initial compliance check, coupled with ongoing monitoring by the competent authorities, is essential to verify that the applicant company is able to ensure and demonstrate continued compliance with the set of data protection standards.

As seen above, under the BCR system, it is up to the competent DPA to approve the data protection policies submitted by the companies. However, considering the resource-constraints to which DPAs are subject, it is worth considering CILP's suggestion to value the role that third-party accountability agents may play in measuring accountability and in certifying that the organizations' privacy program is sound and capable of ensuring adequate protection.[1385] Third-party agents, which remind of the accountability agents under the CBPR system, may hence efficiently supplement the work of data protection authorities in reviewing and approving company's applications and in subsequently overseeing compliance with the approved privacy management program. Indeed, as stressed by the CILP, "[q]ualified, authorised accountability agents will be an important element to address resource constraints in order to make the accountability approach work in practice".[1386] This is even more true considering that, consistently with the CBPR system, according to the CILP, such

[1383] Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 200.
[1384] Ibid., 194, 199 and 208.
[1385] Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 15; Centre for Information Policy Leadership, *Demonstrating and Measuring Accountability. A Discussion Document*, 9.
[1386] Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 15.

third-party agents should not only have "front-line oversight", and hence enforcement powers, but also complaint-handling responsibilities.[1387]

At the same time, as stressed by the CILP, if the proposed accountability-based framework is designed so as to entirely revolve around the assessment conducted by third-party agents, the credibility and reliability of such agents would become an essential cornerstone of the system. This is why specific criteria would need to be developed in order to ensure that these agents can be trusted by both regulators and the public.[1388] In this regard, it should be noted that, under Articles 42 and 43 GDPR, the GDPR already entrusts third parties with the task of issuing and renewing certifications. These third parties are certification bodies "which have an appropriate level of expertise in relation to data protection".[1389] Moreover, the EDPB has already issued guidelines on the accreditation of certification bodies under Article 43 GDPR. These Guidelines aim to help "Member States, supervisory authorities and national accreditation bodies establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR".[1390] The suitability of these certification bodies in measuring accountability and the overall privacy management programs developed by the applicants under the proposed accountability-based system should hence be assessed.

However, and as a more general consideration, it should be noted that the location of the data controller/processor in a third country would generate some administrative and practical problems. Indeed, the physical distance between the certification bodies and the organizations seeking certification may hinder certification bodies' ability to effectively assess whether the third-country applicant meets the certification criteria and subsequently monitor compliance with the certification.

[1387] Centre for Information Policy Leadership, *The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society*, 25–26.

[1388] Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 16–17; Centre for Information Policy Leadership, *Demonstrating and Measuring Accountability. A Discussion Document*, 9.

[1389] Article 43(1) GDPR.

[1390] European Data Protection Board, *Guidelines 4/2018 on the Accreditation of Certification Bodies under Article 43 of the General Data Protection Regulation (2016/679) - Version 3.0*, 2019, 6, accessed December 15, 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf.

As seen above, the CBPR system solves these administrative problems by requiring that the participating APEC Economies nominates at least one Accountability Agent which is in charge of certifying organizations as CBPR compliant (besides having enforcement powers). These practical difficulties may also be overcome by establishing collaborations between certification bodies in the EU and certification bodies in the third country. The certification body in the EU may indeed delegate the local collaborator to perform its tasks on its behalf. In this case the certification bodies in the EU should make sure that the local certification body lives up to the high standards set out under the EU data protection framework for the accreditation of certification bodies.[1391]

Let's now move to the third element, i.e., *enforceability* of the internal privacy policies by *data protection authorities*. As seen above, CBPRs achieve enforceability by means of the tight cross-border cooperation between the different enforcement authorities in the APEC Economies in which transfer takes place, as opposed to BCRs which achieve enforceability by means of an EU centric enforcement mechanism. Starting from the assumption that trusted and "low friction" movement of data between companies located in different jurisdictions "requires that privacy enforcement agencies rely upon the oversight of enforcement bodies in jurisdictions other than their own",[1392] CBPRs seem to offer a useful model for building a "trusted" environment for free flow of data. What makes the CBPR system a useful paradigm is the fact that it operates on a double level: firstly, it seeks guarantees at the country level, since the CBPR framework makes participation of APEC Economies to the system dependant, among others, on having enforcement authorities in place; secondly, it

[1391] "In establishing a collaboration with a local certification body, the certification body established in the EU should seek warranties that the local collaborator lives up to the high standards of the GDPR accreditation requirements of Art. 43, the requirements of the Regulation 765/2008, and the ISO/IEC 17011. In addition, the local certification body should be able to provide certification on the basis of the ISO/IEC 17065. A safe way to ensure high standards is the accreditation of the local certification body (in the third country) by the national accreditation authority of that country participating in the International Accreditation Forum", which is an international association of organizations which promotes agreements between accreditation bodies in different countries and aims to achieve equivalence of accreditations issued by the members of the Forum. Kamara et al., *Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679*, 178.

[1392] Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 4.

requires organizations wishing to join the system to voluntary adopt internal rules, in line with the APEC Privacy Framework, and undergo an independent compliance review.

With the due adjustments, this system seems to be compatible with the EU data protection framework. This system could, indeed, be assimilated to a *partial* adequacy decision, under which adequate protection to the transferred data is offered by a combination of (1) commitments undertaken by organizations in the non-EEA jurisdiction to abide by the EU data protection rules and of (2) domestic legal components which should be present in that jurisdiction in order to ensure the effective implementation of such rules.[1393] This system presents at least two advantages. Firstly, the possibility to rely on the oversight powers of enforcement agencies established in third countries would enable not only intra-group transfers but also *inter*-group transfers. Secondly, since there would be no need for subjecting the non-EEA data recipients to the long arm of the EU regulators, non-EEA certified recipients would have the certainty of dealing with local enforcement authorities. This is relevant since one of the drawbacks of BCRs is that the implementation at the global level of such internal binding rules would put non-EEA affiliates under the monitoring and enforcement powers of the EU DPAs: "[m]any foreign entities do not like or understand this, particularly those with a centre of business outside the EU".[1394]

Overall, it can be concluded that the CBPR system seems to offer a good model for ensuring enforceability of internal privacy policies by including both *voluntary* and *regulatory* components: compliance with the applicable data protection rules is ensured by the privacy policies and practices

[1393] Some authors have indeed assimilated CBPRs to the Privacy Shield rather than to BCRs. Among others, Sullivan (2019) noted that "[m]ost of the transfer mechanisms under GDPR have similarities with CBPR but the latter is most similar in approach to Privacy Shield in that CBPR requires acceptance at country level, followed by an independent certification process for the individual organization wishing to join the scheme". Sullivan, "EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era," 3. Along the same lines, Wall (2017) noted that "[t]he CBPR program is analogous to the EU-U.S. Privacy Shield in that they both provide a means for self-assessment, compliance review, recognition/acceptance and dispute resolution/enforcement. Both systems require the designation by each country of a data protection authority". Alex Wall, "GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules," *Iapp*, May 31, 2017, accessed August 22, 2019, https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/.

[1394] Allen & Overy, *Binding Corporate Rules*, 2016, 9, accessed August 15, 2019, http://www.allenovery.com/SiteCollectionDocuments/BCRs.pdf; Information Integrity Solutions, *Towards a Truly Global Framework for Personal Information Transfers. Comparison and Assessment of EU BCR and APEC CBPR Systems*, 35–36.

established by certified organizations while the enforcement of such rules is ensured by the enforcement authorities established in the jurisdiction(s) in which those certified organizations are established. This model would translate into a sort of a "mixture" of the geographical approach, on which adequacy is based, and of the organization-to-organization approach, which underpins data transfers based on accountability. Under this model, on the one hand, the inefficiencies and ineffectiveness of a full adequacy assessment of third countries' legal order would be replaced by companies' commitments to the applicable data protection principles. On the other hand, geography would retain its importance since companies' commitments would need to be backed up by some minimum requirements embedded within third countries' domestic law.[1395]

Another piece of the puzzle should now be added: since it is well established that organizations should be held accountable not only to regulators but also to data subjects, the fourth element of the proposed system provides that *redress mechanisms* should be made available to data subjects in the event that they are adversely affected by non-compliance with the applicable data protection rules. As suggested by the CILP, and consistently with the criteria for approval of BCRs and with the criteria for participation in CBPR, in order to address individuals' complaints, accountable organizations should implement an internal complaints-handling mechanism in order to make sure that complaints are promptly dealt with. The submission of complaints against non-EU data importers may also be facilitated by EU data exporters and/or by DPAs which may, for example, channel complaints to the non-EU company concerned.

Redress mechanisms would also need to be implemented to solve situations in which data subjects are not satisfied by the replies and the actions taken by the defaulting organization in response to their complaints. In this regard, alternative means of redress should be devised and implemented in order to overcome the limitations of "traditional compliance and enforcement

[1395] A "reconciliation" between the geographical and the organizational approaches was suggested by Kuner as a means to address the fact that, notwithstanding the limits of a data transfer regime based on geography, "geography will continue to play a role in the regulation of transborder data flows". Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, 39–41.

mechanisms (such as fines, investigations by data protection authorities, and court actions)".[1396] In particular, alternative dispute resolution procedures, such as arbitration and mediation, could be set up as a means to overcome the difficulties of asserting rights against companies outside the country of export.[1397]

Overall, the four elements identified above seem to represent useful building blocks for the development of a trusted international environment populated by certified entities among which data could be safely transferred. In this framework, the rules on transborder data flow set out under Chapter V GDPR could apply as soon as data leave this trusted environment: *onward transfer* from certified data recipients to non-certified third parties could hence continue to be regulated by the EU data transfer rules.[1398] This entails that the greater is the number of companies certified under the accountability-based system and of countries which have adhered to the system, the broader would be the area of "low friction" international data transfer. In this framework, on the one hand, data subjects could rely on a common level of protection regardless of data location. On the other hand, regulators would have confidence that personal data collected from data subjects in the EU would continue to be processed in compliance with the high EU data protection standards and that, in case of non-compliance, the defaulting organizations would be subject to the enforcement powers of the competent authorities established in the foreign jurisdiction.

Besides being *desirable*, the development of an accountability-based data transfer regime seems also *feasible*. Indeed, from a *procedural* viewpoint, the proposed regime is built on several

[1396] Organisation for Economic Cooperation and Development, *Report on Compliance with, and Enforcement of, Privacy Protection Online*, 2003, 14, accessed August 24, 2019, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2002)5/FINAL&docLanguage=En.

[1397] "OECD member countries and private sector entities have developed and continue to develop alternative means to ensure compliance with and enforcement of privacy law which go beyond traditional governmental regulations and sanctions ... There is considerable potential for taking existing mechanisms for privacy compliance and enforcement and adapting them to the online environment. For instance, some member countries and commercial entities have made it possible to file privacy-related complaints online, and there are also a number of alternative dispute resolution (ADR) mechanisms for privacy disputes under development". Ibid., 14.

[1398] The same rule applies under BCRs: as soon as data leave the group, adequate protection will need to be provided in compliance with Chapter V GDPR. See Criterion 6.1.1 for approval of BCRs, WP256 rev.01 and criterion 6.1 for approval of BCRs, WP257 rev.01.

existing elements: the concept of accountability is already enshrined in the EU framework as one of the core EU data protection principles as well as in the legal framework of other jurisdictions and it would impose on organizations commitments which resemble the commitments under BCRs. From a *substantive* viewpoint, as stressed by the CILP in the Galway project, accountability is not meant to replace existing regulation. Rather, accountability requires organizations to develop and implement internal data protection policies which reflect external legislation and established best practices.[1399] In other words, the implementation of an accountability-based data transfer regime would not require a complete (and hence unrealistic) rethinking of the norm itself but rather the implementation of measures to ensure compliance and demonstrate compliance with such norms both in intra-EU and international processing operations.[1400]

Despite the desirability and feasibility of the proposed accountability-based certification mechanism, the establishment of a similar regime certainly requires further work and consultations with various stakeholders. As a sort of mid-term goal, efforts to achieve interoperability between BCRs and CBPRs could be intensified. Interoperability could be facilitated by bridging the differences between BCRs and CBPRs with "additional undertakings on the part of the CBPR-certified company, to the extent that is necessary to enable data transfers in and out of the EU". In the longer term, "differences might even be reflected in the rules of the CBPR System itself".[1401] If complete interoperability between the two systems is achieved, the toolbox of legal bases for data transfer could be enriched by recognizing that CBPRs also provide for appropriate safeguards under Article 46 GDPR. Indeed, since Article 26 DPD (now Article 46 GDPR) is worded as an open-ended provision, CBPRs could be included under the list of measures providing appropriate safeguards (together with SCCs, ad hoc contracts and others). What is sure is that the inclusion of CBPRs within

[1399] Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 3, 9.

[1400] Alhadeff, Van Alsenoy, and Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," 71–72.

[1401] Information Integrity Solutions, *Towards a Truly Global Framework for Personal Information Transfers. Comparison and Assessment of EU BCR and APEC CBPR Systems*, 37.

the list under Article 46 GDPR would entail the establishment of a mechanism under which EU supervisory authorities can cooperate with APEC regulators so that complaints coming from one jurisdiction can be investigated and addressed.[1402]

Interoperability between the two systems would certainly be beneficial for companies, especially for those operating on a global scale, since it would allow organizations to develop an internal and *uniform* privacy program which meets the legal requirements of different jurisdictions. Interoperability based on accountability would hence allow the development of "uniform and high level privacy policies, procedures and operational controls for the company" and would "foster a company-wide privacy culture across multiple jurisdictions".[1403] Moreover, interoperability should be promoted not only between CBPRs and BCRs but also between CBPRs and other EU data transfer tools, in particular codes of conduct (Article 40 GDPR) and certifications (Article 42 GDPR)[1404] so that companies that satisfy the requirements under one of these transfer tool should be able to transfer data among themselves without implementing additional requirements.

6.4.4. Conclusion

This chapter has tested three different possible solutions to the limitations that currently hamper the smooth transfer of data from the EU to third countries. Global convergence of data protection standards (solution 1) is certainly the most desirable solution. Indeed, over the years, data protection has acquired a strong international dimension since data constantly flow from one country to another. The harmonization of data protection standards at the international level would hence make data transfer restrictions unnecessary since data would receive the same level of protection regardless of their location. As highlighted above, however, at present there is no legally binding instrument that regulates data protection on a global basis, although some positive steps towards

[1402] Ibid.

[1403] Centre for Information Policy Leadership, *The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society*, 21.

[1404] Centre for Information Policy Leadership, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*, 12.

global convergence have been taken, either formally or informally. On a formal level, Convention 108 seems to be the only existing binding international instrument which holds the potential for growing as a global data protection agreement thanks to its binding nature; thanks to the fact that any country, even non-European countries can adhere to the Convention; thanks to the fact that, together with the GDPR and the 1995 Directive before it, it has inspired the legislative process of many countries around the globe. Moreover, Convention 108 prescribes the appointment of one or more data protection authorities thus specifically addressing enforcement issues which often arise when data are transferred across borders.

On an informal level, *de facto* global convergence has been driven by the EU data protection standards. Indeed, on the one hand, several non-EU countries have adopted, or have started the process of adopting, data protection laws which are clearly inspired by the GDPR. On the other hand, several companies operating at a global level have started to implement GDPR-compliant policies that extend the level of protection guaranteed under the GDPR to non-EU based customers. This *de facto* approximation of the data protection laws of different countries may have some immediate positive effects in boosting international data flow: (1) approximation of the laws is expected to relieve companies operating globally of the compliance challenges they often face when trying to abide by a bewildering number of different legal requirements; (2) States that have adopted GDPR-like data protection legislations are more likely to be found adequate by the European Commission.

This chapter has also examined the alleged unnecessary overlap between rules on transborder data flow and rules on applicable law, i.e., Article 3 GDPR. Indeed, some have argued that data transfer rules should not apply, and data should hence be free to flow to non-EU entities which are directly subject to the GDPR by virtue of its broad territorial scope. The adoption of this approach would certainly boost international data transfers since the transfer to non-EU entities that fall under the extra-territorial scope of the GDPR would be unrestricted. However, as highlighted above, the implementation of data transfer rules still retains an added value in protecting data even if the data recipient is directly subject to the GDPR. Indeed, when data are transferred from EU data controllers

to non-EU data processors, the *in*-direct applicability of the GDPR to non-EU processors which derives from the implementation of DP Agreements seems unsuited to address the specific enforcement challenges that arise when data are transferred outside the EU borders. In other words, DP Agreements seem to be fit for ensuring the *applicability* of GDPR data protection principles but unfit for ensuring the *effective implementation* of such principles.

Along the same lines, when data are transferred to non-EU controllers which directly fall under the scope of Article 3 GDPR, the extraterritorial scope of the GDPR seems to successfully guarantee that the EU data protection rules apply to the data recipient and that transferred data continue to benefit from the same level of protection as in the country of origin. At the same time, however, the implementation of data transfer mechanisms would offer an extra layer of protection in ensuring or, at least, aiming to ensure the effective implementation of the GDPR. In other words, even if Article 3 GDPR seems to successfully expand the applicability of the GDPR beyond the EU borders, data transfer rules would strengthen data protection by coupling the broad, but weak, extraterritorial applicability of the GDPR with some specific procedural and enforcement mechanisms. The added value of data transfer rules should thus be identified in the attempt to link the applicability of data protection rules to their effective implementation. In the light of this, this chapter has highlighted that the need to implement data transfer mechanisms, and hence the need to restrict international data transfer, would be substantially reduced if a system of mutual cooperation is established between the supervisory authorities of EU and non-EU countries. However, although several international and regional frameworks of international cooperation have been established, most of the existing arrangements are non-binding or non-comprehensive.

The last section of the chapter has examined the promising role that the principle of accountability could play in boosting international data flow by increasing *organizational responsibility* in ensuring appropriate safeguards. Several building blocks for an accountability-based data transfer regime have been identified on the basis of the successful experience of BCRs and the promising elements included in CBPRs. The elements that may help frame international data transfers

in a more efficient, flexible and scalable fashion are the following: (1) a *baseline level of data protection* which takes the form of *internal policies* adopted by the companies and which is demonstrated through (2) *initial certification* and *ongoing audit* and which is (3) enforced by *data protection authorities* and (4) via *redress mechanisms* by data subjects.

Data transfer should hence be grounded upon the principle of accountability which would impose onerous obligations on companies wishing to be certified under the system: such obligations boil down to the implementation of a privacy management program and the criteria for approval of such program could be inspired by the essential elements of accountability identified by the CILP. Free flow of data between different regions and jurisdictions would hence be facilitated by encouraging companies to implement internal policies which, consistently with the GDPR, set high standards of data protection. A preliminary check (followed by ongoing verification) by independent third parties in charge of verifying whether the applicants guarantee adequate protection to personal data should also be established. Some guarantees should also be embedded in the third country's legislative framework. In particular, the transfer of data to non-EEA companies should be made dependent upon the presence of enforcement authorities in that foreign jurisdiction, unlike BCRs (which depends on an EU-centric enforcement mechanism) but similarly to CBPRs (which impose several legislative and enforcement requirements on Economies wishing to join the system). This would assimilate the system to a partial adequacy decision in which commitments from organizations are complemented with guarantees embedded in the third country's legal order. Several mechanisms would also need to be implemented in order to ensure effective redress to data subjects. In particular, accountable organizations should implement an internal complaints-handling mechanism in order to make sure that complaints are promptly addressed. Redress mechanisms, such as alternative dispute procedures, should also be established in order to solve situations in which data subjects are not satisfied by the actions taken by the defaulting organization in response to their complaints.

7. Conclusion

This research has attempted to identify the main policy objectives underpinning the EU data transfer rules, their inherent limitations in achieving these objectives and the steps that should be taken to build an international environment populated by entities among which data can flow freely without undermining the EU data protection standards. This research is hence an attempt to reconcile the quest for free flow of data with the legitimate concerns about the risks to which data may be exposed once they are transferred to third-country recipients. The *substance* of the EU data transfer rules (i.e., ensuring continued data protection regardless of data location) should hence be preserved, while new solutions for regulating international data transfer should be "tested".

This study has first located the EU data transfer rules in the broader debate about the challenges that the un-territorial cyberspace places to States' capabilities to exert their control and hence jurisdiction over data (chapter 2); it has then delved into the extent of the territorial scope of the GDPR so as to understand how far the GDPR goes in protecting personal data when data are processed by third-country entities (chapter 3); the objectives underpinning data transfer rules (chapter 4) and the weaknesses of such rules in achieving these objectives (chapter 5) have then been analysed; lastly, all these elements have been taken together so as to identify the steps that should be taken for ensuring a free but safe international transfer of data (chapter 6).

In more detail, chapter 2 has shown that, in a context where economic and social developments largely depend on the unfettered movement of data and where the vast majorities of businesses are enabled by the access and the sharing of information across borders, traditional geographical and political borders still retain a great deal of importance. States around the world have, indeed, adopted data localization measures which aim to control, and hence restrict, data entering and leaving their territory. EU data transfer rules, as an essential component of the EU data protection framework, are part of this trend. Indeed, these rules mirror the EU attempt to exert and extend its jurisdiction over

data as a means to ensure that the level of protection guaranteed within the EU is not undermined once data leave the EU.

Chapter 3 has analysed the territorial scope of the GDPR and, in particular, its extra-territorial applicability to companies that have no (or very weak) physical presence in the EU. In reading Article 3, and considering the restrictions that chapter V of the GDPR places on international transfer of data, it may come as a surprise that the physical location of personal data (and the location of the processing activities) is immaterial for determining the applicability of the EU data protection legislation. The location of the file as a connecting factor for triggering the EU jurisdiction was indeed dropped from the original proposal back in the nineties since it was clear that processing operations could have more than one location. Under the GDPR, other connecting factors were chosen: the establishment of a controller or of a processor in the European Union (and the loose boundaries of the concept of "establishment" and of what may represent an "inextricable link" between the activities of the EU establishment and the data processing activities of the non-EU data controller); the targeting criterion (and the difficulties of uncovering the subjective intention of non-EU companies offering goods or services to data subjects in the EU); the monitoring criterion (and the risk that any company with an online presence may be exposed to the strict obligations under the EU data protection legislation).

It has been noted that the broad extra-territorial scope of the GDPR is certainly motivated by a laudable purpose: ensuring effective and complete protection of the right to privacy. At the same time, chapter 3 has also highlighted the negative consequences that inevitably arise when the jurisdictional grounds are designed and interpreted in such a broad and flexible fashion: conflicts of law, uncertainties about the extent of the obligations to which companies are subject, and the problems of enforceability that are likely to accompany any attempts to implement the EU legislation outside the EU borders. The adoption of a more "cautious" approach was hence suggested in interpreting and applying the jurisdictional grounds set out under Article 3 GDPR. In particular, it has been argued that the gap between applicability and enforceability that is likely to derive from an excessively broad extra-territorial scope of the GDPR could be filled by applying the GDPR only

"where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved".[1405] Since enforcement actions are the tool that have the greatest effect on influencing the behaviours of commercial actors, the overall level of compliance with EU data protection rules by non-EEA entities could be increased by tightening the link between applicability and enforceability. In this respect, enforceability problems may be partly solved by the obligation under Article 27 GDPR to appoint a representative within the EU. Indeed, even if EU representatives shall not be held directly liable for any misdemeanour committed by the non-EU entity, DPAs can *address* to the EU representatives enforcement actions which are *directed* to the non-EU data controller or processor they represent.

Chapter 4 has delved into the very basics of data transfer rules, firstly, by investigating the objectives that underpin such rules, secondly, by composing the puzzle of the concept of "transfer". The chapter has shown that two main rationales underpin data transfer rules: on the one hand, ensuring that the level of protection from which individuals in the EU benefit in relation to the processing of their personal data is not undermined once data leave the EU; on the other hand, ensuring that data are not exposed to disclosure requests by foreign public authorities which go beyond what is necessary in a democratic society. The chapter has then looked into the definitional problems that affect the very notion of "transfer". In the absence of an official definition of the concept of transfer, some elements that characterize the said concept can be identified: transfer is generally understood as the *physical movement* of data from one country to another; it involves the presence of a *recipient* that is subject to the jurisdiction of the receiving country; it is normally understood, yet mistakenly,[1406] as implying communication and hence *disclosure* of data to the recipient; "transfer" within the scope of the GDPR differs from "making data publicly available" online since it involves the transmission of data to some *identified* individuals and not to *anyone* with an Internet connection;

[1405] Article 29 Data Protection Working Party, *WP56*, 9.

[1406] As seen in chapter 4 (4.3.), encrypted data are still personal data. This entails that provisions on international data transfer need to be complied with even if the EEA data controller/processor sends encrypted data to the non-EEA data controller/processor. In this case, even if the non-EEA data controller/processor will *not* have (intelligible) access to the data, the data transfer rules will need to be complied with.

transfer also differs from transit since data transfer provisions only apply when data are meant to be further processed in the receiving non-EEA country and not when data are merely routed through a non-EEA country without being processed in any way.

Chapter 5 has analysed in depth the data transfer provisions under the GDPR so as to understand their practical functioning, as well as their limitations in enabling a smooth and safe international data transfer. The chapter has shown that no substantial changes have been introduced by the Regulation although some new legal bases have been added to the "toolkit for international transfers" and others (i.e., BCRs) have been formalized. As outlined in the chapter, several limitations still affect the transfer mechanisms set out under the Regulation. Among others, the adequacy of the level of protection offered by the Privacy Shield has been called into question by many parties with reference to both the commercial aspects and the potential generalised access to the transferred data by US public authorities. Moreover, other structural problems affect this legal basis for transfer: the process of adopting adequacy decisions is notoriously lengthy and its focus on geography makes them particularly unfit for transfers in the cloud where many geographical locations are involved. The fact that adequacy decisions can now also be adopted with reference to a specific territory or a sector within a third country should however be welcomed since different sectors or regions within the same country may be covered by different laws, some of which may be found adequate even if the system as a whole is not.

Moving from Article 45 to Article 46 GDPR, it is worth recalling standard contractual clauses which are widely used in practice. However, as seen throughout the chapter, the implementation of SCCs is often impractical for framing international data transfer in a context where multiple parties and multiple countries are involved and SCCs for processor-to-processor transfers are yet to be adopted. Overall, SCCs have proved to lack the necessary adaptability and flexibility that is required to meet the different and constantly changing scenarios of modern international data transfers. SCCs should hence be revised so as to make their structure more flexible and adaptable to the complexity

of modern data processing operations, for example, by enabling the signing by multiple parties, whether data processors or data controllers.

Together with SCCs, it is worth recalling BCRs which have proved to be more than a tool for framing international data transfers. Indeed, they do not only allow to carry out multiple transfers between multiple companies of the same group by means of a single instrument, but they also serve as a *global* standard for data protection that all group companies are required to implement. At the same time, however, their approval process faces several bureaucratic challenges, and BCRs can only be used for intra-group transfers or for transfer within a "group of enterprises engaged in a joint economic activity" (whatever that means). Moreover, the same concerns about access to data for surveillance and/or enforcement purposes that have been expressed with reference to the Privacy Shield can be extended to SCCs and BCRs. The data recipients may, indeed, be required to disclose data to public authorities and such requests inevitably take precedence over any contractual obligation.

Moving from "old" to "new" legal bases for transfer, it has been argued that the possibility to resort to codes of conduct and certification mechanisms as new legal bases for transfers seems promising. Indeed, on the one hand, codes of conduct may not only serve as an international data transfer tool but also as a medium for promoting and spreading internationally the EU standards for data protection. On the other hand, certification mechanisms have the potential of substantially boosting international data flow since they allow EEA companies to easily identify non-EEA companies that have been certified as providing appropriate safeguards. At the same time, certified non-EEA companies, especially SMEs, could easily "signal" their reliability to EEA companies wishing to export data outside the EU. However, questions remain about how these legal bases for transfer will develop in practice and how efficient they will actually be in boosting international data flow. Derogations under Article 49 GDPR were also examined: in the absence of adequacy decisions and of appropriate safeguards, companies may rely on the derogations set out under Article 49 GDPR. These derogations should, however, be interpreted and applied in a manner that preserves their nature

of exception to the general rules under Articles 44-47 GDPR. This derives from the fact that derogations do not guarantee that data subjects will continue to enjoy the same level of protection they are afforded in the EU and should hence be applied as a last resort. Overall, the exceptional nature of the derogations under Article 49 GDPR seems incompatible with data transfers in the cloud where the flow of data is more likely to be "repetitive" than exceptional.

Lastly, a whole range of unanswered questions arise when trying to make sense of how data transfer regime for processors works in practice. The need for safety valves has been highlighted in this respect. In particular, it has been argued that the EU data transfer rules should not apply in situations where there is a very limited connection with the EU and where the applicability of the EU data protection rules seems even to against the intention of the EU legislators. In particular, it has been argued that in a scenario where data about non-EU individuals are collected and processed by a non-EU data controller which does not fall under Article 3 GDPR and which engages a data processor in the EU, data transfer rules should not apply to the transfer from the EU processor to the non-EU data controller. The implementation of data transfer rules in a similar scenario would, indeed, lead to the *indirect* application of EU data protection rules in situations where the *direct* applicability of the EU data protection regime has been excluded by the EU legislators.

The chapter has then examined data transfer rules in the light of the objectives underpinning such rules so as to answer the following question: *how effective are* data transfer rules *in achieving their underpinning objectives?* Firstly, the analysis has shown that the relationship between Article 3 of the GDPR and data transfer restrictions is unclear. Indeed, it has been highlighted that the implementation of data transfer mechanisms seems redundant in achieving the anticircumvention objective when the processing of transferred data directly falls under the scope of the GDPR by virtue of its extraterritorial reach. Secondly, data export restrictions – we could say, data protection law more broadly – seem powerless in restraining access from third-country public authorities for national security and/or law enforcement reasons. Moreover, recent developments, both within and outside the EU, show that data location is increasingly losing its relevance as a connecting factor for

grounding data disclosure requests in both the law enforcement and the intelligence fields. A delineation should hence be drawn between rules on government access to data and data transfer rules for commercial purposes: a balance between privacy and security is certainly necessary but data transfer rules for commercial purposes do not seem to be the appropriate place for achieving such balance. *Ad hoc* international discussions seem hence necessary in this respect.

After having examined the main limitations of the existing data transfer rules, chapter 6 aimed at identifying the building blocks for a more flexible and scalable data transfer system. In identifying these building blocks for achieving a "data free flow with trust"[1407], the analysis has been guided by the desire to strike a balance between the need to show a "reasonable degree of pragmatism in order to allow interaction with other parts of the world"[1408] and the need to assert the value of the right to data protection as a fundamental human right.[1409] Three possible "solutions" have been tested. These solutions are based, respectively, on (1) global convergence; (2) the role that rules on applicable law may play in making data transfer rules "superfluous", and (3) the principle of accountability.

Global convergence of data protection standards (solution 1) is certainly the most desirable way forward. Indeed, if one of the main objectives underpinning data export restrictions is to avoid the circumvention of EU data protection law, there would be no need to restrict international data flow if data are transferred to a country that affords an "essentially equivalent" level of protection. The analysis conducted in the chapter has, however, shown that *informal* and hence *de facto* global convergence seems to be more promising than *formal* global convergence by means of internationally agreed standards. Indeed, at present, there is no legally binding instrument that regulates data protection on a global basis and the chances of achieving a truly international data protection treaty

[1407] *G20 Osaka Leaders' Declaration*.

[1408] Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, n.d., 43, accessed January 5, 2020, https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf.

[1409] In his opinion on *Schrems II,* the Advocate General stated that his "analysis as a whole will be guided by the desire to strike a balance between, on the one hand, the need to show a 'reasonable degree of pragmatism in order to allow interaction with other parts of the world', and, on the other hand, the need to assert the fundamental values recognised in the legal orders of the Union and its Member States, and in particular in the Charter". Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, *Facebook Ireland and Schrems*, Case C-311/18, paragraph 7.

in the next few years appear fairly slim although some hopes rest with Convention 108 +. Moreover, it has been argued that even if true globalisation of Convention 108 + were to be achieved, its standards may not meet the high threshold of protection set out under the European data protection framework. More generally, any global standard is likely to be limited to some general principles while detailed rules are likely to be left to secondary legislation which, instead of requiring international consensus, can be quickly amended "if changing circumstances so require".[1410] Besides being unfeasible (at least in the next few years), the adoption of a binding international agreement may, to some extent, even be undesirable. Indeed, on the one hand, data protection rules mirror different cultural values so that bridging differences in privacy legislations would also entail bridging cultural differences. On the other hand, some developing countries may value the economic opportunities offered by the Internet more than protection from privacy risks so that the adoption of high (i.e., strict) data protection standards may prematurely hamper the development of their economy. Among other possible international fora, the potentials of trade agreements in facilitating data flow have also been explored. However, the analysis has found that the European Commission, as well as other European institutions, is committed to exclude data protection from trade negotiations: trade agreements can be a powerful means for contrasting unjustified data localization requirements but they are ill-suited to deal with data protection as a fundamental human right.

At the same time, the past forty years have witnessed a sort of *de facto* approximation of the laws of different countries with more and more non-European countries adopting privacy laws close to the European standards. Moreover, the adoption at the national level of GDPR-like data protection rules has been coupled with the adoption by companies of GDPR-compliant policies across their global processing operations regardless of the legal obligation to do so. Several companies have, indeed, started of their own volition to implement and expand the level of protection guaranteed by the GDPR to non-EU based customers. Even in the absence of internationally agreed data protection

[1410] Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, 67.

standards, this gradual convergence may boost international data transfer in, at least, two ways. Firstly, the development of common data protection rules may relieve companies operating globally of the compliance challenges that they often face when trying to navigate between divergent national data protection requirements. Secondly, the adoption by third countries of GDPR-like data protection acts and the ratification of Convention 108 may indirectly boost international data transfer by easing the adoption of adequacy decisions on the part of the European Commission.

The chapter has also examined the claim advanced by many parties under which data transfer provisions seem to be unnecessary when data are transferred to companies that are caught under Article 3 GDPR. Indeed, when the processing of data entirely falls under the territorial scope of the GDPR, the purpose of data transfer provisions (i.e., avoiding the circumvention of the EU data protection legislation) seems to be already achieved by the rules on applicable law. The analysis conducted in the chapter has, however, shown that the implementation of data transfer rules still retains an added value in ensuring compliance with the EU data protection standards. Two scenarios have been examined: (1) the transfer of data from an EEA data controller to a non-EEA data processor and (2) the transfer of data from an EEA data controller to a non-EEA data controller. In order to answer the question whether the implementation of data transfer rules adds any value in protecting data when the data recipient is already subject to the application of the GDPR, the two requirements against which the adequacy of data transfer solutions should be assessed have been taken into account: compliance with the substantive data protection rules set out in the EU framework on the one hand and the presence of procedural/enforcement mechanisms which make those rules effective on the other.

In the first scenario (transfer of data from an EEA data controller to a non-EEA data processor), the applicability of data protection rules is ensured by the DP Agreements that shall be stipulated pursuant to Article 28 GDPR (regardless of the processor's location). At the same time, the analysis has shown that, even if no real circumvention risk can be envisaged since processors are bound to follow the controller's instructions, data transfer rules complement the *applicability* of the

EU data protection principles with mechanisms that ensure the *enforceability* of such principles by both data subjects and DPAs. Indeed, outside the EU, in most cases there is no guarantee that procedural means for ensuring compliance with data protection rules are in place thus raising potential enforcement problems for both data subjects and DPAs. Data transfer rules hence specifically aim to compensate for the deficiencies in the protection afforded by third countries by granting data subjects redress (and hence enforceability of their data protection rights) and by ensuring the possibility of intervention by data protection authorities. Moreover, as stressed in several parts of the present research, when data are transferred to entities located in third countries, the non-EEA data recipient may be required by the law to which it is subject to disclose data to public authorities. For this reason, data transfer rules also include information requirements under which data recipients should inform the data exporter of disclosure requests and of other events which may prevent them from ensuring the guarantees provided under the data transfer tool. These information requirements would hence allow data exporters and supervisory authorities to retain (some) control over the transferred data by prohibiting or suspending the transfer.

Similarly, when data are transferred to non-EEA data controllers that are directly subject to the GDPR, the EU data protection rules will certainly be applicable to the relevant processing activities simply by virtue of the broad (extra)territorial scope of the Regulation. At the same time, data transfer rules may translate into an *indirect* way of ensuring the *effective* implementation of the GDPR (or, at least, of its basic principles) by complementing the *direct* applicability of the GDPR with some enforcement mechanisms. Indeed, bearing in mind the enforcement problems that arise from the unilateral extra-territorial expansion of the EU jurisdiction to third-country entities, it has been argued that the implementation of data transfer provisions would strengthen the direct (but weak) applicability of the GDPR thanks to specific enforcement and procedural mechanisms (e.g., third party beneficiary rights; liability clauses; duties of cooperation with DPAs; provisions aimed at addressing the problem of overriding laws). This would ensure that at least some basic data protection principles are not only applicable but also made effective.

Long story short, the added value of data transfer rules in protecting transferred data should be identified in the attempt to link the applicability of data protection rules to their effective implementation. In the light of this, it has been argued that the need to implement data transfer mechanisms would become less compelling if a system a mutual cooperation is established between EEA and non-EEA supervisory authorities. Mutual assistance between supervisory authorities would, indeed, help bridge the gap between the applicability of data protection principles and their effective implementation. Some frameworks of international cooperation among supervisory authorities have already been established both on bilateral and multilateral levels. However, since existing cooperation mechanisms are not effective as they should be due to their non-binding and/or non-comprehensive nature, the possibilities for cross-border cooperation between supervisory authorities should be strengthened.

The third, and last, section of the chapter aimed at identifying the possible foundations for a data transfer regime built on the concept of "accountability" as it has been developed not only within the EU framework but also in other jurisdictions. Indeed, the principle of accountability, as an instrument of data governance, seems to play a promising role in boosting international data transfer in the way it pushes most of the burden for ensuring compliance *on* organizations and *away* from resource-constrained regulators. In particular, it has been argued that the CBPR system includes, and shares with the BCR system, several features which seem to be suitable for framing a free but safe flow of data among different jurisdictions: (1) a *baseline level of data protection* which takes the form of *internal policies* adopted by companies and which is demonstrated through (2) *initial certification* and *ongoing audit* and which is (3) enforced by *data protection authorities* and (4) via *redress mechanisms* by data subjects.

Firstly (element 1), the proposed data transfer system should be based on a baseline level of data protection which takes the form of internal policies. These internal policies should mirror the provisions established in the GDPR while also including organizational arrangements designed to put such provisions into effect along the lines of BCR requirements. In order to address the limitations

of existing data transfer rules, the proposed system would hence place on companies most of the responsibility for ensuring compliance with data protection legislation by developing GDPR-compliant privacy management programs. The development of privacy management programs seems also to be consistent with the increasing efforts undertaken by businesses in implementing GDPR-compliant policies for their worldwide processing operations (the so-called "GDPR-creep"). Secondly (element 2), a preliminary check (followed by ongoing verification) by means of certification by independent third parties should also be established. Initial certification and ongoing oversights would, on the one hand, put companies under the obligation to *demonstrate* their compliance with the applicable data protection rules to the competent authority, and, on the other, allow the competent authority (i.e., the DPAs or third-party agents) to verify whether the applicants guarantee adequate protection to personal data.

The third requirement (element 3) aims to ensure that the *voluntary* components of the proposed system (i.e., the privacy management programs adopted by the "certified" companies) are backed up by some *regulatory* components. Indeed, while the *applicability* of data protection rules can be ensured by companies' commitments (i.e., their internal privacy management programs), the *enforceability* of such rules would need to be ensured by the powers of enforcement authorities. The proposed system hence aims to seek guarantees at the country level by requiring that the transfer of data to third-country companies is dependent upon the presence in that third country of enforcement authorities. This system could so be assimilated to a *partial* adequacy decision: commitments from organizations to abide by EU data protection standards are complemented with guarantees embedded in the third country's legal order and aimed at ensuring the effective implementation of those standards. Lastly (element 4), in order to ensure accountability not only to supervisory authorities but also to data subjects, redress mechanisms should be made available to data subjects which have been adversely affected by non-compliance with the applicable data protection rules.

The development of an accountability-based data transfer regime would certainly require further work. At the same time, the feasibility of this regime rests with the fact that its implementation

would not require a complete rethinking of data protection rules, but the implementation of a *procedural* scheme designed to ensure compliance with such rules across companies' worldwide processing operations. It has also been argued that, as a sort of "mid-term" goal, efforts to achieve the interoperability between existing EU and non-EU data transfer tools should be intensified.

In the meantime, it should be noted that instead of devising a *new* data transfer regime, the European Commission seems to be more committed to harness the full potentials of *existing* data transfer tools. To this end, the European Commission is engaging with several third countries with the view of reaching new adequacy decisions and it is committed to modernize SCCs in the light of the new requirements set out under the GDPR and of business needs and practices. Moreover, the European Commission has asked the EDPB to intensify its work on the possible solutions for streamlining the approval process for BCRs, to finalise its guidance on codes of conduct and certification mechanisms and, notably, to clarify the interplay between the rules on international data transfer and the extra-territorial scope of the GDPR. As regards the international dimension, the European Commission is committed to promote convergence of data protection laws at different international fora and to support ongoing reform processes in third countries which may ultimately lead to the adoption of adequacy decisions. Moreover, it has recognized the importance of strengthening cooperation and mutual assistance between EU and foreign privacy enforcers as a means to "bring convergence 'from the books to the ground'"[1411] and is engaging in international negotiations to this end.[1412] Besides developing and strengthening bilateral tools, the European Commission seems also to be keen to explore whether a multinational framework can be established so as to allow data to flow freely among like-minded countries "while ensuring the required level of protection on the basis of shared values and converging systems".[1413]

[1411] 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. (Brussels, 2020), 14, accessed July 7, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

[1412] Ibid., 10–18.

[1413] 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. (Brussels, 2019),

Against this background, and leaving for a moment aside the – still far to be reached – possibility to build international data transfer on the basis of global convergence (solution 1), the conclusions reached in chapter 6 may take the current framework (and its likely developments in the light of the European Commission's agenda) some steps further in developing the toolkit for data transfers. First, if effective implementation of the applicable rules across borders is achieved (in particular by means of enforcement cooperation between EEA and non-EEA supervisory authorities), we could argue that the gap between the applicability and the enforceability of data protection rules that has been highlighted in the second part of chapter 6 (solution 2) would be filled. This may lead to the (tentative) conclusion that the transfer of data to recipients which are already (directly or indirectly) subject to the GDPR may be truly superfluous and that data should be free to flow to those non-EEA recipients. Second, as argued in the third part of chapter 6 (solution 3), the accountability principle and the commitments undertaken by businesses in implementing GDPR-compliant policies (i.e., internal privacy management programs), if backed up with a certification system and with some regulatory elements enshrined in third countries' jurisdiction, should be valued and further elaborated as a promising means to ensure continued and enforceable GDPR compliance regardless of data location.

12, accessed July 7, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0374&from=EN.

Bibliography

27th International Conference of Data Protection and Privacy Commissioners. *Montreux Declaration - The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities*. Montreux, 2005. https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf.

30th International Conference of Data Protection and Privacy Commissioners. *Resolution on the Urgent Need for Protecting Privacy in a Borderless World, and for Reaching a Joint Proposal for Setting International Standards on Privacy and Personal Data Protection*. Strasbourg, 2008. Accessed June 8, 2019. http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resoltuion-on-the-urgent-need-for-protecting-privacy-in-a-borderless-world.pdf.

31st International Conference of Data Protection and Privacy Commissioners. *International Standards on the Protection of Personal Data and Privacy*. Madrid, 2009. Accessed April 15, 2019. http://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf.

39th International Conference of Data Protection and Privacy Commissioners. *Resolution on Exploring Future Options for International Enforcement Cooperation*. Hong Kong, 2017. Accessed December 22, 2019. http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-exploring-future-options-for-International-Enforcement-Cooperation-2017.pdf.

41st International Conference of Data Protection and Privacy Commissioners. *Resolution on the Conference's Strategic Direction (2019-21)*. Tirana, 2019. Accessed December 22, 2019. https://privacyconference2019.info/wp-content/uploads/2019/10/Resolution-on-the-Conference-Strategic-Direction-2019-2021-FINAL.pdf.

Aaditya, Mattoo, and Meltzer Joshua P. *International Data Flows and Privacy. The Conflict and Its Resolution*, 2018. http://documents.worldbank.org/curated/en/751621525705087132/pdf/WPS8431.pdf.

Adhikari, Richard. "Deutsche Telekom Pitches NSA-Free German Internet." *TechNewsWorld*. Last modified October 26, 2013. Accessed January 3, 2018. https://www.technewsworld.com/story/79286.html.

Ahmed, Murad. "Amazon to Open German Data Centres to Soothe European Concerns." *Financial Times*. Last modified October 23, 2014. Accessed February 16, 2018. https://www.ft.com/content/56181a6e-5a96-11e4-b449-00144feab7de.

Albright Stonebridge Group. *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, 2015. Accessed January 22, 2018. https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf.

Alhadeff, Joseph, Brendan Van Alsenoy, and Jos Dumortier. "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions." In *Managing Privacy through Accountability*, edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland, and Hector Postigo, 49–82. London: Palgrave Macmillan, 2012.

Allen & Overy. *Binding Corporate Rules*, 2016. Accessed August 15, 2019. http://www.allenovery.com/SiteCollectionDocuments/BCRs.pdf.

American Chamber of Commerce to the European Union. *Our Position - Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, 2019. Accessed May 2, 2019. http://www.amchameu.eu/system/files/position_papers/amchameu_edpb_guidelines_on_territorial_scope.pdf.

Ango, Michael, and Samuel Ibrahim. “Data Protection Regulation 2019: An Emerging Frontier in Data Management in Nigeria.” *Andersen Tax Digest*, April 23, 2019. Accessed June 5, 2019. https://andersentax.ng/data-protection-regulation-2019-an-emerging-frontier-in-data-management-in-nigeria/.

APEC. *Cooperation Arrangement Cross-Border Privacy Enforcement*. Hiroshima, Japan: 2010/SOM1/ECSG/DPS/013, 2010. Accessed April 15, 2019. http://mddb.apec.org/documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf.

Article 29 Data Protection Working Party. *Adequacy Referential (Updated) (WP254)*, 2017. Accessed December 15, 2019. https://iapp.org/media/pdf/resource_center/wp254_Adequacy-referential_11-2017.pdf.

———. *EU – U.S. Privacy Shield – First Annual Joint Review (WP255)*, 2017.

———. *Explanatory Document on the Processor Binding Corporate Rules (WP204 Rev.01)*, 2015. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf.

———. *FAQs in Order to Address Some Issues Raised by the Entry into Force of the EU Commission Decision 2010/87/EU 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 (WP176)*, 2010. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf.

———. *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy (WP4)*, 1997. Accessed January 2, 2020. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf.

———. *Guidelines on Consent under Regulation 2016/679 (WP259 Rev.01)*, 2018. Accessed December 15, 2019. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

———. *Opinion 1/2001 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Article 26(4) of Directive 95/46 (WP38)*, 2001. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp38_en.pdf.

———. *Opinion 1/2008 on Data Protection Issues Related to Search Engines (WP148)*, 2008. Accessed January 2, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.

———. *Opinion 1/2010 on the Concepts of “Controller” and “Processor” (WP169)*, 2010. Accessed January 2, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

———. *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision (WP238)*, 2016. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

———. *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 (WP212)*, 2014. Accessed December 23, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf.

———. *Opinion 3/2009 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC (Data Controller to Data Processor) (WP161)*, 2009. Accessed December 15, 2019.

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp161_en.pdf.

———. *Opinion 3/2010 on the Principle of Accountability (WP173)*, 2010. Accessed December 27, 2019. https://www.dataprotection.ro/servlet/ViewDocument?id=654.

———. *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes (WP215)*, 2014. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

———. *Opinion 04/2016 on European Commission Amendments Proposals Related to the Powers of Data Protection Authorities in Standard Contractual Clauses and Adequacy Decisions (WP241)*, 2016. Accessed December 15, 2019. https://iapp.org/media/pdf/resource_center/wp241_Opinion-EC_DPAs-SCCs-adequacy.pdf.

———. *Opinion 05/2012 on Cloud Computing (WP196)*, 2012. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

———. *Opinion 7/2001 on the Draft Commission Decision (Version 31 August 2001) on Standard Contractual Clauses for the Transfer of Personal Data to Data Processors Established in Third Countries under Article 26(4) of Directive 95/46 (WP47)*, 2001. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp47_en.pdf.

———. *Opinion 8/2003 on the Draft Standard Contractual Clauses Submitted by a Group of Business Associations ("the Alternative Model Contract") (WP84)*, 2003. Accessed January 6, 2020. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp84_en.pdf.

———. *Opinion 8/2010 on Applicable Law (WP179)*, 2010. Accessed January 2, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf.

———. *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128)*, 2006. Accessed January 2, 2020. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf.

———. *Sixteenth Report – Covering the Year 2012*, 2014. Accessed December 15, 2019. https://cnpd.public.lu/dam-assets/en/publications/rapports/groupe29/16th_annual_report_en.pdf.

———. *Statement on the Decision of the European Commission on the EU-U.S. Privacy Shield*, 2016. Accessed December 15, 2019. 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.

———. *Working Document 01/2014 on Draft Ad Hoc Contractual Clauses "EU Data Processor to Non-EU Sub-Processor" (WP214)*, 2014. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf.

———. *Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection through Surveillance Measures When Transferring Personal Data (European Essential Guarantees) (WP237)*, 2016. Accessed January 2, 2020. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

———. *Working Document 02/2012 Setting up a Table with the Elements and Principles to Be Found in Processor Binding Corporate Rules (WP195)*, 2012. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

———. *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP114)*, 2005. Accessed December 8, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf.

———. *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites (WP56)*, 2002. Accessed January 2, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf.

———. *Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes (WP228)*, 2014. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.

———. *Working Document: Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries (WP9)*, 1998. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp9_en.pdf.

———. *Working Document Setting Forth a Co-Operation Procedure for the Approval of "Binding Corporate Rules" for Controllers and Processors under the GDPR (WP263 Rev.01)*, 2018. Accessed December 15, 2019. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056.

———. *Working Document Setting up a Table with the Elements and Principles to Be Found in Binding Corporate Rules (WP153)*, 2008. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf.

———. *Working Document Setting up a Table with the Elements and Principles to Be Found in Binding Corporate Rules (WP256 Rev.01)*, 2018. Accessed December 15, 2019. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

———. *Working Document Setting up a Table with the Elements and Principles to Be Found in Processor Binding Corporate Rules (WP257 Rev.01)*, 2018. Accessed December 15, 2019. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

———. *Working Document: Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (WP74)*, 2003. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf.

———. *Working Document. Transfers of Personal Data to Third Countries. Applying Articles 25 and 26 of the EU Data Protection Directive (WP12)*, 1998. Accessed December 15, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf.

Article 29 Data Protection Working Party, and Working Party on Police and Justice. *The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data (WP168)*, 2009. Accessed December 26, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf.

Azzi, Adèle. “The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation.” *Journal of Intellectual Property, Information Technology and E-Commerce Law* 9, no. 2 (2018). Accessed April 19, 2019. https://www.jipitec.eu/issues/jipitec-9-2-2018/4723/JIPITEC_9_2_2018_126_Azzi.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” *Electronic Frontier Foundation*. Last modified January 20, 2016. Accessed January 31, 2018. https://www.eff.org/it/cyberspace-independence.

Bartoli, Emmanuelle. *Data Transfers in the Cloud: Discussion Paper for the Commission’s Expert Group on Cloud Computing Contracts*, 2014. Accessed August 3, 2018. https://docplayer.net/4162422-Data-transfers-in-the-cloud.html.

Bauer et al., Matthias. *The Costs of Data Localisation: Friendly Fire on Economic Recovery*. ECIPE occasional paper No. 3/2014, 2014. Accessed February 11, 2019. https://ecipe.org/publications/dataloc/.

Bauer, Matthias, Fredrik Erixon, Michal Krol, and Hosuk Lee-Makiyama. *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*. ECIPE, 2013. Accessed January 24, 2018. https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

Bauer, Matthias, Martina F. Ferracane, Hosuk Lee-Makiyama, and Erik van der Marel. *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States*. ECIPE, Policy Brief No. 03/2016, 2016. Accessed November 2, 2019. https://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/.

Beiter, Katie. “Iran Introduces Halal Internet.” *The Media Line*, September 8, 2016. Accessed January 2, 2018. http://www.themedialine.org/news/iran-introduces-halal-internet/.

Bender, David. “Having Mishandled Safe Harbor, Will the CJEU Do Better with Privacy Shield? A US Perspective.” *International Data Privacy Law* 6, no. 2 (May 1, 2016): 117–138.

Bennett, Colin. “International Privacy Standards: Can Accountability Be Adequate?” *Privacy Laws & Business International Newsletter*, no. 106 (August 2010): 21–23. Accessed August 21, 2019. https://dspace.library.uvic.ca/bitstream/handle/1828/10394/Bennett_Colin_PrivLawsBusiness_Aug%202010.pdf?sequence=1.

———. “The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?” *Information Polity* 23 (2018): 239–246. Accessed May 28, 2019. https://pdfs.semanticscholar.org/3813/041fc44467933d64c54c3e39a467c2be63c3.pdf.

Bildt, Carl. “One Net, One Future.” *Centre for International Governance Innovation*. Last modified October 26, 2015. Accessed January 26, 2018. https://www.cigionline.org/articles/one-net-one-future.

Bilgic, Secil. “Something Old, Something New, and Something Moot: The Privacy Crisis Under the Cloud Act.” *Harvard Journal of Law & Technology* 32, no. 1 (2018): 321–355.

Bioni, Bruno, Maria Cecília Oliveira Gomes, and Renato Leite Monteiro. “GDPR Matchup: Brazil’s General Data Protection Law.” *Iapp*, October 4, 2018. Accessed May 24, 2019. https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/.

Bird & Bird LLP. *Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009.

Bitkom. *Views on EDPB Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)*, 2019. Accessed May 2, 2019. https://www.bitkom.org/sites/default/files/2019-

01/20190118_Bitkom%20Position%20Paper%20EDPB%20Guidelines%20on%20the%20Territorial%20Scope%20%283%29.pdf.

Blume, Peter. "Transborder Data Flow: Is There a Solution in Sight?" *International Journal of Law and Information Technology* 8, no. 1 (January 1, 2000): 65–86.

Borrud, Gabriel. "Germany Looks to Erect IT Barrier." *Deutsche Welle*. Last modified November 4, 2013. Accessed January 3, 2018. http://www.dw.com/en/germany-looks-to-erect-it-barrier/a-17203480.

Bortnick, Jane. "International Information Flow: The Developing World Perspective." *Cornell International Law Journal* 14, no. 2 (1981): 333–353.

Böse, Martin. *An Assessment of the Commission's Proposals on Electronic Evidence*, 2018. Accessed May 7, 2019. http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf.

Bowman, Courtney M. "A Primer on Russia's New Data Localization Law." *Privacy Law Blog*. Last modified August 27, 2015. Accessed December 31, 2017. https://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/.

———. "Data Localization Laws: An Emerging Global Trend." *JURIST*. Last modified January 6, 2017. Accessed January 18, 2018. http://www.jurist.org/hotline/2017/01/Courtney-Bowman-data-localization.php.

Box, Sarah. *Internet Openness and Fragmentation: Toward Measuring the Economic Effects*. Global Commission on Internet Governance, Paper Series No. 36, 2016. Accessed January 25, 2018. https://www.cigionline.org/sites/default/files/gcig_no.36_web.pdf.

Boyle, Emma. "UN Declares Online Freedom to Be a Human Right That Must Be Protected." *The Independent*. Last modified July 5, 2016. Accessed January 26, 2018. http://www.independent.co.uk/life-style/gadgets-and-tech/un-declares-online-freedom-to-be-a-human-right-that-must-be-protected-a7120186.html.

Brown, Ian. "The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance." *International Journal of Law and Information Technology* 23, no. 1 (2015): 23–40.

Bryan Cave Leighton Paisner Data Privacy and Security Team. "Complying with the EU General Data Protection Regulation (GDPR): Cross Border Transfers of Information," Celesq® AttorneysEd Center, May 1, 2018. Accessed April 23, 2019. https://www.bclplaw.com/images/content/1/0/v2/103150/gdpr-5-1-2018.pdf.

Bughin, Jacques, and Susan Lund. "The Ascendancy of International Data Flows." *McKinsey Global Institute*, January 9, 2017. Accessed December 29, 2019. https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows.

Busch, Andreas. "The Regulation of Privacy." *Jerusalem Papers in Regulation & Governance, Working Paper No. 26* (2010): 1–22. Accessed February 7, 2018. http://regulation.huji.ac.il/papers/jp26.pdf.

Business Roundtable. *Framework for Consumer Privacy Legislation*, 2018. Accessed May 25, 2019. https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf.

———. *Promoting Economic Growth through Smart Global Information Technology Policy. The Growing Threat of Local Data Server Requirements*, 2012. Accessed January 25, 2018. http://businessroundtable.org/sites/default/files/Global_IT_Policy_Paper_final.pdf.

Business Software Alliance. *The Software Alliance's Response to the EDPB Public Consultation on the Proposed Guidelines on the Territorial Scope of the GDPR*. Brussels, 2019. Accessed May 2, 2019. https://www.bsa.org/sites/default/files/2019-02/01182019BSAResponseEDPBPublicConsultationonProposedGuidelinesonTerritorialScopeofGDPR.pdf.

Buttarelli, Giovanni. "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard." *International Data Privacy Law* 6, no. 2 (2016): 77–78.

———. "The EU-U.S. Privacy Shield Two Years On." *European Data Protection Supervisor*. Last modified March 26, 2018. Accessed May 30, 2018. https://edps.europa.eu/press-publications/press-news/blog/eu-us-privacy-shield-two-years_en.

Bygrave, Lee A. "European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation." *Computer Law & Security Review* 16, no. 4 (August 1, 2000): 252–257.

———. "International Agreements to Protect Personal Data." In *Global Privacy Protection: The First Generation*, edited by James B. Rule and Graham Greenleaf, 15–49. Cheltenham: Edward Elgar, 2008.

Carroll, Rory. "Google's Worst-Kept Secret: Floating Data Centers off US Coasts." *The Guardian*, October 30, 2013. Accessed April 7, 2018. http://www.theguardian.com/technology/2013/oct/30/google-secret-floating-data-centers-california-maine.

Carson, Angelique. "Merck First Company to Win BCRs via APEC's CBPRs." *Iapp*, March 22, 2016. Accessed August 20, 2019. https://iapp.org/news/a/merck-first-company-to-win-bcrs-via-apecs-cbprs/.

Carvalho, Isabel, and Rafael Loureiro. "Brazil Creates a Data Protection Authority." *HL Chronicle of Data Protection*. Last modified January 11, 2019. Accessed May 24, 2019. https://www.hldataprotection.com/2019/01/articles/international-eu-privacy/brazil-creates-a-data-protection-authority/.

Centre for Information Policy Leadership. "A New Approach to International Transfers in Response to the European Commission's Communication on 'A Comprehensive Approach to Personal Data Protection.'" In *Accountability: A Compendium for Stakeholders*, 2011. Accessed August 10, 2019. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders__march_2011_.pdf.

———. *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*, 2017. Accessed August 25, 2019. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

———. *Comments on the European Data Protection Board's "Draft Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)" Adopted on 16 November 2018*, 2019. Accessed May 3, 2019. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_edpbs_territorial_scope_guidelines.pdf.

———. *Data Protection Accountability: The Essential Elements. A Document for Discussion*, 2009. Accessed August 5, 2019. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_protection_accountability-the_essential_elements__discussion_document_october_2009_.pdf.

———. *Demonstrating and Measuring Accountability. A Discussion Document*, 2010. Accessed August 9, 2019. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/demonstrating_and_measuring_accountability_a_discussion_document__accountability_phase_ii-the_paris_project_october_2010_.pdf.

———. *Implementing Accountability in the Marketplace A Discussion Document*, 2011. Accessed August 25, 2019. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/implementing_accountability_in_the_marketplace__accounrtability_phase_iii-the_madrid_project_november_2011_.pdf.

———. *Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR*, 2019. Accessed December 9, 2019. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_paper_on_key_issues_relating_to_standard_contractual_clauses_for_international_transfers_and_the_way_forward_for_new_standard_contractual_clauses_under_the_gdpr.pdf.

———. *The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society*, 2018. Accessed August 25, 2019. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

Chander, Anupam, and Uyên P. Lê. "Data Nationalism." *Emory Law Journal* 64 (2015): 677–739. Accessed January 7, 2018. http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

Chansanchai, Athima. "Microsoft Research Project Puts Cloud in Ocean for the First Time." *Microsoft Stories*, February 1, 2016. Accessed April 7, 2018. https://news.microsoft.com/features/microsoft-research-project-puts-cloud-in-ocean-for-the-first-time/.

Choo, Kim-Kwang Raymond, Russell G. Smith, and Rob McCusker. *Future Directions in Technology-Enabled Crime: 2007–09*. Research and Public Policy Series No. 78, Australian Institue of Criminology, 2007. Accessed January 23, 2018. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.4136&rep=rep1&type=pdf.

Chuffart-Finsterwald, Stéphanie. "Data Protection in Switzerland: Overview." *Practical Law*. Last modified July 1, 2016. Accessed January 18, 2018. https://uk.practicallaw.thomsonreuters.com/9-502-5369?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

Chui, Wing Hong. "Quantitative Legal Research." In *Research Methods for Law*, edited by Michael McConville and Chui, 48–71. Second edition. Edinburgh: Edinburgh University Press, 2017.

City of London Law Society Data Law Committee. *Submission to the European Data Protection Board on Guidelines 3/2018*, 2019. Accessed May 2, 2019. http://www.citysolicitors.org.uk/attachments/category/186/CLLS%20Consultation%20Response%20on%20EDPB%20Territorial%20Scope%20Guidelines.pdf.

Clark, James, and Natalie Webb. "ICO Clarifies Position in Respect of International Transfers under the GDPR." *Privacy Matters - DLA Piper*, September 12, 2018. Accessed February 8, 2019. https://blogs.dlapiper.com/privacymatters/uk-ico-clarifies-position-in-respect-of-international-transfers-under-the-gdpr/.

Clarke, John. "Data-Processing Agreements from 30,000 Feet." *Iapp*, May 22, 2018. Accessed March 7, 2019. https://iapp.org/news/a/data-processing-agreements-from-30000-feet/.

Cohen, Bret, Britanie Hall, and Charlie Wood. "Data Localization Laws And Their Impact on Privacy, Data Security And the Global Economy." *Antitrust* 32, no. 1 (2017): 107–114. Accessed February 15, 2018. https://www.perkinscoie.com/en/news-insights/data-localization-laws-and-their-impact-on-privacy-data-security.html.

Colonna, Liane. "Article 4 of the EU Data Protection Directive and the Irrelevance of the EU–US Safe Harbor Program?" *International Data Privacy Law* 4, no. 3 (2014): 203–221.

Commission of the European Communities. *Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. COM(92)422 final, 1992. Accessed April 12, 2018. http://aei.pitt.edu/10375/1/10375.pdf.

———. *Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data*. COM(90) 314 final-SYN 287 and 288. Brussels, 1990. Accessed November 24, 2019. http://aei.pitt.edu/3768/1/3768.pdf.

Cook, Tim. "Remarks before the International Conference of Data Protection & Privacy Commissioners," Brussels, Belgium, October 24, 2018. Accessed May 24, 2019. https://www.privacyconference2018.org/system/files/2018-10/Tim%20Cook%20speech%20-%20ICDPPC2018.pdf.

Cooper, Daniel, and Hilary Wandall. "Scaling Data Protection Globally through Interoperable Accountability." *Datenschutz und Datensicherheit - DuD* 41, no. 2 (February 1, 2017): 74–76.

Cory, Nigel. *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* Information Technology and Innovation Foundation, 2017. Accessed January 1, 2018. http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.188877538.836303334.1505916541-133641866.1498770015.

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*. Strasbourg: ETS No. 181, 2001.

———. *Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal?*, 2010. Accessed February 11, 2019. https://rm.coe.int/16802fa3df.

———. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Strasbourg: ETS No.108, 1981.

———. *European Convention on Human Rights*. CETS No. 005, 1950.

———. *Explanatory Report to the 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*. Strasbourg: ETS No. 181, 2001.

———. *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Strasbourg: CETS No. 223, 2018.

———. *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Strasbourg: CETS No. 223, 2018.

———. *The Modernised Convention 108: Novelties in a Nutshell*, n.d. Accessed May 20, 2019. https://rm.coe.int/16808accf8.

Council of Europe, and Committee of Ministers. *Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector*, 1987.

Council of Europe, Cybercrime Convention Committee. *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*. Strasbourg, 2014. Accessed

February 21, 2018. https://rm.coe.int/16802e726c.

Council of the European Union. *3430th Council Meeting, Outcome of the Council Meeting*. Brussels, 2015. Accessed June 7, 2019. http://data.consilium.europa.eu/doc/document/ST-14688-2015-INIT/en/pdf.

———. *Council Decision Authorising the Opening of Negotiations with a View to Concluding 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*. Brussels, 2019. Accessed December 14, 2019. https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf.

———. *Council Position and Findings on the Application of the General Data Protection Regulation (GDPR)*. Brussels, 2019. Accessed December 29, 2019. https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf.

———. *Outcome of the Council Meeting*. 3622nd Council meeting, Justice and Home Affairs, 9680/18. Luxembourg, 2018. Accessed May 7, 2019. https://www.consilium.europa.eu/media/35542/st09680-en18.pdf.

———. *The Stockholm Programme – An Open and Secure Europe Serving and Protecting the Citizens*. Brussels, 2009. Accessed June 10, 2016. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/the_stockholm_programme_-_an_open_and_secure_europe_en_1.pdf.

Cromption, Malcolm. "East Meets West: Striving to Interoperable Frameworks?" *Data Protection Law & Policy* (May 2014): 11–13. Accessed August 22, 2019. https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f62d08a65e232a6959d2b/1465869010281/IIS+Crompton+Shao+DPLP+May+2014+-+BCR+CBPR.pdf.

Cryer, Robert, Tamara Hervey, Bal Sokhi-Bulley, and Alexandra Bohm. *Research Methodologies in EU and International Law*. 1st ed. Oxford: Hart Publishing, 2011.

Daskal, Jennifer. "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0." *Stanford Law Review Online* 71, no. 9 (2018): 9–16. Accessed May 6, 2019. https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.

———. "The Un-Territoriality of Data." *The Yale Law Journal* 125 (2015): 326–398. Accessed January 31, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2578229.

Daskal, Jennifer, and Peter Swire. "Why the CLOUD Act Is Good for Privacy and Human Rights." *Lawfare*, March 14, 2018. Accessed May 6, 2019. https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

Data Guidance, and Future of Privacy Forum. *Comparing Privacy Laws: GDPR v. CCPA*, 2018. Accessed May 26, 2019. https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

Deloitte. *Value of Connectivity: Economic and Social Benefits of Expanding Internet Access*, 2014. Accessed January 24, 2018. https://www2.deloitte.com/view/en_GB/uk/industries/tmt/extending-internet-access/index.html.

Digital Europe. *Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009. Accessed August 12, 2019. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/digital_europe_en.pdf.

———. *Response to Public Consultation on EDPB Draft Guidelines on Territorial Scope*. Brussels, 2019. Accessed May 2, 2019. https://www.digitaleurope.org/wp/wp-

content/uploads/2019/01/DIGITALEUROPE-response-to-EDPB-territorial-scope-guidelines-FINAL.pdf.

Dobinson, Ian, and Francis Johns. “Legal Research as Qualitative Research.” In *Research Methods for Law*, edited by Michael McConville and Wing Hong Chui, 18–47. Second edition. Edinburgh: Edinburgh University Press, 2017.

Dockery, Stephen. “Data Localization Takes Off as Regulation Uncertainty Continues.” *The Wall Street Journal*, June 6, 2016. Accessed November 2, 2019. https://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/.

Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwächter. *Internet Fragmentation: An Overview*. Future of the Internet Initiative White Paper, World Economic Forum, 2016. Accessed February 20, 2018. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Dunn, Jeff. “The Tech Industry Is Dominated by 5 Big Companies — Here’s How Each Makes Its Money.” *Business Insider Italia*, May 29, 2017. Accessed January 15, 2018. http://www.businessinsider.com/how-google-apple-facebook-amazon-microsoft-make-money-chart-2017-5.

Dutch DPA. *Publication of Personal Data on the Internet*, 2007. Accessed May 14, 2018. https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_20071108_richtsnoeren_internet.pdf.

Dutta, Soumitra, William H. Dutton, and Ginette Law. *The New Internet World, A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online*. INSEAD Working Paper No. 2011/89/TOM, 2011. Accessed January 29, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1916005.

Eger, John M. “Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers.” *Law and Policy in International Business* 10 (1978): 1055–1103.

Ehlers, Rachel E. “The Data Care Act of 2018.” *The National Law Review*, December 27, 2018. Accessed May 25, 2019. https://www.natlawreview.com/article/data-care-act-2018.

European Commission. *5th Round of Trade Negotiations between the European Union and Indonesia - EU Provisions on Cross-Border Data Flows and Protection of Personal Data and Privacy in the Digital Trade Title of EU Trade Agreements*, 2018. Accessed June 30, 2020. https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf.

———. “Adequacy of the Protection of Personal Data in Non-EU Countries.” Accessed May 26, 2018. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

———. *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 (2010/87/EU)*. OJ L 39/5, 2010.

———. *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, 2001.

———. *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 (2002/2/EC)*. OJ L 2/13, 2001.

———. *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, 2000.

———. *Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC*. OJ L 6/52, 2001.

———. *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 (2004/915/EC)*. OJ L 385/74, 2004.

———. *Commission Decision of 30 June 2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina*. OJ L 168/19, 2003.

———. *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*. OJ L 207/1, 2016.

———. *Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 Amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the Adequate Protection of Personal Data by Certain Countries, Pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council 25(6) of Directive 95/46/EC of the European Parliament and of the Council*. OJ L 344/83, 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 344/100, 2016.

———. *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, 2019.

———. *Commission Staff Working Document. Impact Assessment, Accompanying the Document 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 Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*. SWD(2018) 118 final. Brussels, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN.

———. *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. Brussels, 2020. Accessed July 7, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

———. *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. Brussels, 2019. Accessed July 7, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0374&from=EN.

———. *Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World*. COM(2017) 7 final. Brussels, 2017. Accessed April 15, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

———. *Communication from the Commission to the European Parliament and the Council. Time to Establish a Modern, Fair and Efficient Taxation Standard for the Digital Economy*. COM(2018) 146 final. Brussels, 2018. Accessed June 22, 2020. https://eur-lex.europa.eu/resource.html?uri=cellar:2bafa0d9-2dde-11e8-b5fe-01aa75ed71a1.0017.02/DOC_1&format=PDF.

———. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union*. COM(2010) 609 final. Brussels, 2010. Accessed May 29, 2019. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.

———. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. "Building A European Data Economy."* COM(2017) 9 final. Brussels, 2017. Accessed June 5, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN.

———. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Trade for All Towards a More Responsible Trade and Investment Policy*. COM(2015) 497 final. Brussels, 2015. Accessed June 5, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0497&from=ga.

———. *Communication from the European Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*. COM(2013) 847 final. Brussels, 2013. Accessed April 26, 2019. https://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF.

———. *EU-New Zealand Free Trade Agreement - Digital Trade Title*, 2018. Accessed July 1, 2020. https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf.

———. *Explanatory Memorandum - Recommendation for a Council Decision Authorising 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. Brussels, 2019. Accessed May 7, 2019. https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf.

———. "Fair Taxation of the Digital Economy." Last modified September 20, 2017. Accessed June 22, 2020. https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en.

———. *First Report on the Implementation of the Data Protection Directive (95/46/EC)*. COM(2003) 265 final. Brussels, 2003. Accessed December 28, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN.

———. *Frequently Asked Questions: New EU Rules to Obtain Electronic Evidence*. Brussels, 2018. Accessed May 7, 2019. http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm.

———. *Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements)*, 2018. Accessed June 28, 2020. https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

———. *Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission*. Tokyo, 2018. Accessed August 1, 2018. https://http://europa.eu/rapid/press-release_STATEMENT-18-4548_en.htmec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_4548.

———. *Notice to Stakeholders. Withdrawal of the United Kingdom from the Union and EU Rules in the Field of Data Protection*, 2018. Accessed December 8, 2019. https://ec.europa.eu/info/sites/info/files/file_import/data_protection_en.pdf.

———. *Political Declaration Setting out the Framework for the Future Relationship between the European Union and the United Kingdom (2019/C 384 I/02)*. OJ C 384I/178, 2019. Accessed June 25, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12019W/DCL(01)&from=EN.

———. *Position Paper on the Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date*, 2017. Accessed December 8, 2019. https://ec.europa.eu/commission/sites/beta-political/files/data_and_protection.pdf.

———. *Proposal for a Council Directive Laying down Rules Relating to the Corporate Taxation of a Significant Digital Presence*. Brussels: COM(2018) 147 final, 2018.

———. *Proposal for a Council Directive on the Common System of a Digital Services Tax on Revenues Resulting from the Provision of Certain Digital Services*. Brussels: COM(2018) 148 final, 2018.

———. *Proposal for a Directive of the European Parliament and of the Council Laying down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*. COM/2018/226 final - 2018/0107 (COD), 2018.

———. *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), 2018.

———. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*. COM(2012) 11 final. Brussels, 2012. Accessed November 24, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.

———. *Proposal for the EU-Australia Free Trade Agreement - Digital Trade Title*, 2018. Accessed June 30, 2020. https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf.

———. "Questions and Answers on a Fair and Efficient Tax System in the EU for the Digital Single Market." Accessed June 22, 2020. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_2141.

———. *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. Brussels, 2017. Accessed April 26, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0611&from=EN.

———. *Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*. COM(2018) 860 final. Brussels, 2018. Accessed April 26, 2019. https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf.

———. *Report from the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield*. Brussels, 2019. Accessed December 8, 2019. https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf.

———. *Report on the 7th Round of Negotiations between the EU and Chile for the Modernisation of the Trade Part of the EU Chile Association Agreement*, 2020. Accessed June 1, 2020. https://trade.ec.europa.eu/doclib/docs/2020/june/tradoc_158772.pdf.

European Commission - Expert Group on Trade Agreements. *Meeting Report of 11 July 2018*, 2018. Accessed July 1, 2020. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=15690.

European Commission - MEMO. "LIBE Committee Vote Backs New EU Data Protection Rules." Last modified October 22, 2013. Accessed March 24, 2018. http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

European Commission - Press release. "European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows." Last modified January 23, 2019. Accessed May 10, 2019. http://europa.eu/rapid/press-release_IP-19-421_en.htm.

———. "European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows." Last modified November 27, 2013. Accessed June 7, 2019. http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

———. "Questions and Answers: Mandate for the EU-U.S. Cooperation on Electronic Evidence." Last modified February 5, 2019. Accessed May 9, 2019. http://europa.eu/rapid/press-release_MEMO-19-863_en.htm.

———. "Security Union: Commission Facilitates Access to Electronic Evidence." Last modified April 17, 2018. Accessed May 9, 2019. http://europa.eu/rapid/press-release_IP-18-3343_en.htm.

———. "Towards a More Dynamic Transatlantic Area of Growth and Investment." Last modified October 29, 2013. Accessed June 7, 2019. http://europa.eu/rapid/press-release_SPEECH-13-867_en.htm?locale=en.

European Council. *European Council Meeting (18 October 2018) - Conclusions*. EUCO 13/18. Brussels, 2018. Accessed May 7, 2019. https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf.

European Data Protection Board. *EU-U.S. Privacy Shield - Second Annual Joint Review*, 2019. Accessed December 15, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf.

———. *First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities*, 2019. Accessed December 26, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

———. *Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation - Version 3.0*, 2019. Accessed December 10, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf.

———. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - Version 2.0*, 2019. Accessed December 15, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf.

———. *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, 2018. Accessed December 15, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

———. *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 - Version 1.0*, 2020. Accessed July 8, 2020. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v1.pdf.

———. *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version 2.0*, 2019. Accessed December 15, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf.

———. *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - Version for Public Consultation*, 2018. Accessed December 15, 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

———. *Guidelines 4/2018 on the Accreditation of Certification Bodies under Article 43 of the General Data Protection Regulation (2016/679) - Version 3.0*, 2019. Accessed December 15, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf.

———. *Information Note on Data Transfers under the GDPR in the Event of a No-Deal Brexit*, 2019. Accessed December 8, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexit_en.pdf.

———. *Opinion 4/2019 on the Draft Administrative Arrangement for the Transfer of Personal Data between European Economic Area ("EEA") Financial Supervisory Authorities and Non-EEA Financial Supervisory Authorities*, 2019. Accessed December 10, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/2019-02-12-opinion_2019-4_art.60_esma_en.pdf.

———. *Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Art. 70.1.b)*, 2018. Accessed December 15, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf.

———. *Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan*, 2018. Accessed December 15, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/2018-12-05-opinion_2018-28_art.70_japan_adequacy_en.pdf.

———. *Oral Pleading before the Court of Justice of the EU Case C-311/18 (Facebook Ireland and Schrems)*, 2019. Accessed December 8, 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/20190709edpbpleadingschremsii_-_for_publication.pdf.

———. *Work Program 2019/2020*, 2019. Accessed January 6, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf.

European Data Protection Supervisor. *Guidelines on the Concepts of Controller, Processor and Joint Controllership under Regulation (EU) 2018/1725*, 2019. Accessed January 2, 2019. https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf.

———. *Information Note on International Data Transfers after Brexit*, 2019. Accessed December 8, 2019. https://edps.europa.eu/sites/edp/files/publication/19-07-16_for_translation_note_on_personal_data_transfers_post-brexit_en.pdf.

———. *Leading by Example: The EDPS Strategy 2015-2019*, 2015. Accessed June 1, 2019. https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf.

———. *Opinion 2/2019 on the Negotiating Mandate of an EU-US Agreement on Cross-Border Access to Electronic Evidence*, 2019. Accessed December 15, 2019. https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf.

———. *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, 2016.

———. *Opinion on the Data Protection Reform Package*, 2012. Accessed November 30, 2019. https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

———. *Position Paper - The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies*. Brussels, 2014. Accessed December 15, 2019. https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf.

———. *Replies to a Request for Cooperation or Consultation under Articles 24(b) Respectively 46(d) of Regulation (EC) 45/2001 Concerning the Publication of Personal Data on the Internet and the Applicability or Not of Article 9 of the Regulation*. Brussels, 2007. Accessed May 13, 2018. https://edps.europa.eu/sites/edp/files/publication/07-02-13_commission_personaldata_internet_en.pdf.

European Data Protection Supervisor, and European Data Protection Board. *Initial Legal Assessment of the Impact of the US CLOUD Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-Border Access to Electronic Evidence*. Brussels, 2019. Accessed December 14, 2019. https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.

European Parliament. *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))*, 2015. Accessed June 28, 2020. https://www.europarl.europa.eu/doceo/document/TA-8-2015-0252_EN.pdf.

———. *Position of the European Parliament Adopted at First Reading on 12 March 2014 with a View to the Adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (EP-PE_TC1-COD(2012)0011)*, 2014. Accessed April 16, 2018. https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TC+P7-TC1-COD-2012-0011+0+DOC+PDF+V0//EN.

———. *Resolution of 3 February 2016 Containing the European Parliament's Recommendations to the Commission on the Negotiations for the Trade in Services Agreement (TiSA)*. 2015/2233(INI), 2016. Accessed January 6, 2019. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0041_EN.pdf.

———. *Resolution of 5 July 2018 on the Adequacy of the Protection Afforded by the EU-US Privacy Shield*. 2018/2645(RSP), 2018. Accessed February 12, 2019. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf?redirect.

———. *Resolution of 6 April 2017 on the Adequacy of the Protection Afforded by the EU-US Privacy Shield*. 2016/3018(RSP), 2016. Accessed August 2, 2018. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0131_EN.pdf?redirect.

———. *Resolution of 12 December 2017 on "Towards a Digital Trade Strategy."* 2017/2065(INI), 2017. Accessed June 28, 2020. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf.

———. *Resolution of 13 December 2018 on the Adequacy of the Protection of Personal Data Afforded by Japan*. 2018/2979(RSP), 2018. Accessed January 14, 2019. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0529_EN.html?redirect.

———. *Resolution of 26 May 2016 on Transatlantic Data Flows*. 2016/2727(RSP), 2016. Accessed August 2, 2018. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0233_EN.pdf?redirect.

European Parliament, and Committee on Civil Liberties Justice and Home Affairs. *Draft Motion for a Resolution, to Wind up the Debate on the Statement by the Commission Pursuant to Rule 123(2) of the Rules of Procedure on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield*. 2018/2645(RSP), 2018. Accessed August 2, 2018. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht. *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*. COM (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 2012. Accessed April 11, 2018. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

European Parliament, and Council of the 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*. OJ L 281/31, 1995.

———. *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*. OJ L 119/89, 2016.

———. *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data*. OJ L 8/1, 2000.

———. *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 (General Data Protection Regulation)*. OJ L 119/1, 2016.

———. *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*. OJ L 295/39, 2018.

European Union Agency for Fundamental Rights, and Council of Europe. *Handbook on European Data Protection Law*. Luxembourg, 2014. Accessed November 30, 2019. https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

European Union Agency for Fundamental Rights, Council of Europe, and European Data Protection Supervisor. *Handbook on European Data Protection Law*, 2018. Accessed May 17, 2019. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.

European Union Ministers. *Global Information Networks: Realising the Potential*. Bonn, 1997. Accessed June 9, 2019. http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm.

Evans, Alex. "Can Germany Really Keep Bytes within Its Borders?" *The Local*, November 29, 2013. Accessed January 3, 2018. https://www.thelocal.de/20131129/german-email-providers-unite-german-internet-against-nsa.

Ezell et al., Stephen J. *Localization Barriers to Trade: Threat to the Global Innovation Economy*. The Information Technology & Innovation Foundation, 2013. Accessed January 22, 2018. http://www2.itif.org/2013-localization-barriers-to-trade.pdf.

Feldman, Mark B., and David R. Johnson. "National Regulation of Transborder Data Flows." *North Carolina Journal of International Law and Commercial Regulation* 7, no. 1 (1982): 1–25.

Fernandez, Diego. "Argentina's New Bill on Personal Data Protection." *Iapp*, October 2, 2018. Accessed May 29, 2019. https://iapp.org/news/a/argentinas-new-bill-on-personal-data-protection/.

Ferracane, Martina Francesca. "How Data Localisation Wipes out the Security of Your Data." *Security Europe*, n.d. Accessed February 16, 2018. http://www.securityeurope.info/how-data-localisation-wipes-out-the-security-of-your-data/.

Finocchiaro, Giusella. "La Giurisprudenza Della Corte Di Giustizia in Materia Di Dati Personali Da Google Spain a Schrems." In *La Protezione Transnazionale Dei Dati Personali. Dai "Safe Harbour Principles" al "Privacy Shield,"* edited by Giorgio Resta and Vincenzo Zeno-Zencovich, 113 – 135. Roma: Roma Tre-press, 2016.

———. "L'accountability Nel Regolamento Europeo." In *Commentario Del Codice Civile Delle Persone*, edited by Angelo Barba and Stefano Pagliantini, 513–524. Milano: Utet Giuridica, 2019.

Fischer, Philipp E. "Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing." *Journal of Intellectual Property, Information Technology and E-Commerce Law* 3, no. 1 (May 15, 2012): 33–59. Accessed June 10, 2019. http://www.jipitec.eu/issues/jipitec-3-1-2012/3321.

Fleischer, Peter. "Call for Global Privacy Standards." *Google Public Policy Blog*, September 14, 2007. Accessed May 23, 2019. https://publicpolicy.googleblog.com/2007/09/call-for-global-privacy-standards.html.

Foitzik, Piotr. "How to Comply with Provisions on Joint Controllers under the GDPR." *Iapp*, September 26, 2017. Accessed February 11, 2019. https://iapp.org/news/a/how-to-comply-with-provisions-on-joint-controllers-under-the-gdpr/.

Fox, Eleanor M. "Extraterritorial Jurisdiction, Antitrust, and the EU Intel Case: Implementation, Qualified Effects, and the Third Kind Essays." *Fordham International Law Journal* 42, no. 3 (2019): 981–998.

Franzese, Patrick W. "Sovereignty in Cyberspace: Can It Exist?" *Air Force Law Review* 64, no. 1 (2009): 1–42. Accessed January 30, 2018. https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist.

Fraser, Erica. “Data Localisation and the Balkanisation of the Internet.” *SCRIPTed* 13, no. 3 (December 2016): 359–373. Accessed December 30, 2017. https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/.

Gabel, Detlev, and Tim Hickman. “Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation.” *White & Case LLP International Law Firm*. Last modified September 13, 2017. Accessed January 16, 2019. https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection.

Gallo, William, and Tra Mi. “New Vietnam Law Bans News Stories From Social Media Sites.” *VOA News*. Last modified August 2, 2013. Accessed January 2, 2018. https://www.voanews.com/a/new-vietnam-law-bans-news-stories-from-social-media-sites/1722190.html.

Garante per la Protezione dei dati personali. *Authorisation to CONSOB for Entering into an Administrative Agreeement for the Transfer of Personal Data between the EEA Financial Supervisory Authorities and the Non-EEA Financial Supervisory Authorities (9119857)*, 2019. Accessed December 15, 2019. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9119857.

Gensler, Lauren. “The World’s Largest Retailers 2017: Amazon & Alibaba Are Closing In On Wal-Mart.” *Forbes*. Last modified May 24, 2017. Accessed January 15, 2018. https://www.forbes.com/sites/laurengensler/2017/05/24/the-worlds-largest-retailers-2017-walmart-cvs-amazon/.

Gerber, David J. “Beyond Balancing: International Law Restraints on the Reach of National Laws.” *Yale Journal of International Law* 10 (1984): 185–221.

Geringer, Stefanie. “National Digital Taxes – Lessons from Europe.” *South African Journal of Accounting Research* (March 23, 2020): 1–19.

Global Privacy Enforcement Network. *Action Plan for the Global Privacy Enforcement Network*, 2012. Accessed April 15, 2019. https://www.privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen.

Goldstein, Doron S., Megan Hardiman, Matthew R. Baker, and Joshua A. Druckerman. “Understanding the EU-US ‘Privacy Shield’ Data Transfer Framework.” *Journal of Internet Law* 20, no. 5 (2016): 18–22.

Government of Canada. “Strengthening Privacy for the Digital Age - Innovation for a Better Canada.” Last modified May 21, 2019. Accessed August 31, 2019. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

Greenberg, Marc H. “A Return to Lilliput: The LICRA v. Yahoo - Case and the Regulation of Online Content in the World Market.” *Berkeley Technology Law Journal* 18, no. 4 (2003): 1191–1258. https://scholarship.law.berkeley.edu/btlj/vol18/iss4/6.

Greenleaf, Graham. *Accountability Without Liability: ‘To Whom’ and ‘With What Consequences’? (Questions for the 2019 OECD Privacy Guidelines Review)*. UNSW Law Research Paper No. 19-67, 2019. Accessed August 22, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384427.

———. *APEC’s Cross-Border Privacy Rules System: A House of Cards?* UNSW Law Research Paper No. 2014-42, 2014. Accessed August 22, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468782.

———. *Convention 108+ and the Data Protection Framework of the EU*. UNSW Law Research Paper No. 18-39, 2018. Accessed May 22, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202606.

———. *Data Protection Convention 108 Accession Eligibility: 80 Parties Now Possible*, 2017. Accessed May 30, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062415.

———. *'European' Data Privacy Standards Implemented in Laws Outside Europe*. UNSW Law Research Paper No. 18-2, 2017. Accessed May 30, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3096314.

———. "Five Years of the APEC Privacy Framework: Failure or Promise?" *Computer Law & Security Review* 25, no. 1 (2009): 28–43.

———. *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*. UNSW Law Research Paper No. 17-45, 2017. Accessed May 29, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035.

———. *International Data Privacy Agreements after the GDPR and Schrems*. UNSW Law Research Paper No. 2016-29, 2016. Accessed May 31, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764864.

———. *Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles*. UNSW Law Research Paper No. 18-53, 2018. Accessed August 22, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3219728.

———. *'Modernised' Data Protection Convention 108 and the GDPR*. UNSW Law Research Paper No. 19-3, 2018. Accessed May 22, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3279984.

———. "'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?" *Computer Law & Security Review* 29, no. 4 (2013): 430–436.

———. *Renewing Data Protection Convention 108: The COE's 'GDPR Lite' Initiatives*. UNSW Law Research Paper No. 17-3, 2016. Accessed May 30, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2892947.

———. *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*. UNSW Law Research Paper No. 2013-40, 2013. Accessed May 31, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877.

———. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108." *International Data Privacy Law* 2, no. 2 (2012): 68–92.

———. *The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'The Right to Privacy in the Digital Age' to the UN High Commissioner for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy*. UNSW Law Research Paper No. 18-24, 2018. Accessed May 22, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3159846.

———. *The UN Special Rapporteur: Advancing a Global Privacy Treaty?* UNSW Law Research Paper No. 2015-69, 2015. Accessed May 17, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2672549&download=yes##.

Gribakov, Andrei. "Cross-Border Privacy Rules in Asia: An Overview." *Lawfare*. Last modified January 3, 2019. Accessed August 19, 2019. https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview.

GSMA. *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC Can Protect Data and Drive Innovation*, 2018. Accessed November 1, 2019. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.

Harris, Leslie. “Don’t Gerrymander the Internet.” *Index on Censorship*, November 4, 2013. Accessed February 16, 2018. https://www.indexoncensorship.org/2013/11/dont-gerrymander-internet/.

Heimes, Rita. “Top 10 Operational Impacts of the GDPR: Part 9 - Codes of Conduct and Certifications.” *Iapp*, February 24, 2016. Accessed January 17, 2019. https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/.

von Heinegg, Wolff Heintschel. “Territorial Sovereignty and Neutrality in Cyberspace.” *International Law Studies* 123, no. 89 (2013): 123–156. Accessed January 30, 2018. http://stockton.usnwc.edu/cgi/viewcontent.cgi?article=1027&context=ils.

de Hert, Paul, and Michal Czerniawski. “Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context.” *International Data Privacy Law* 6, no. 3 (July 13, 2016): 230–243.

Heyder, Markus. “The APEC Cross-Border Privacy Rules—Now That We’ve Built It, Will They Come?” *Iapp*, September 4, 2014. Accessed August 23, 2019. https://iapp.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come/.

Hill, Jonah Force. “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders.” *Lawfare Research Paper Series* 2, no. 3 (2014): 1–41. Accessed December 30, 2017. https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf.

Hogan Lovells. *International Data Transfers. Considering Your Options*, 2015. Accessed August 2, 2018. https://www.hldataprotection.com/files/2015/10/HL-International-Data-Transfers-Considering-your-options.pdf.

Hon, W. Kuan. *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens*. Cheltenham, UK: Edward Elgar Publishing, 2017.

Hon, W. Kuan, Julia Hörnle, and Christopher Millard. “Which Law(s) Apply to Personal Data in Clouds?” In *Cloud Computing Law*, edited by Christopher Millard, 220–249. Oxford: Oxford University Press, 2013.

Hon, W. Kuan, and Christopher Millard. “How Do Restrictions on International Data Transfers Work in Clouds?” In *Cloud Computing Law*, 254–282. Oxford: Oxford University Press, 2013.

Hon, W. Kuan, Christopher Millard, Chris Reed, Jatinder Singh, Ian Walden, and Jon Crowcroft. *Policy, Legal and Regulatory Implications of a Europe-Only Cloud*. Legal Studies Research Paper 191/2015, Queen Mary University of London, School of Law, 2015. Accessed May 4, 2018. http://www.picse.eu/sites/default/files/PolicyLegalandRegulatoryImplicationsof%20EuropeOnlyCloud.pdf.

Hondius, Frits W. “Data Law in Europe.” *Stanford Journal of International Law* 16, no. 2 (1980): 87–111.

Howell, Catherine, and Darrell M. West. “The Internet as a Human Right.” *Brookings*, November 7, 2016. Accessed January 26, 2018. https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/.

Hustinx, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, n.d. Accessed January 5, 2020. https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf.

Hutt, Rosamond. “The World’s Most Popular Social Networks, Mapped.” *World Economic Forum*. Last modified March 20, 2017. Accessed January 15, 2018. https://www.weforum.org/agenda/2017/03/most-popular-social-networks-mapped/.

Information Commissioner's Office. "Accountability and Governance." Accessed December 27, 2019. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.

———. "Information Rights and Brexit Frequently Asked Questions." Accessed June 25, 2020. https://ico.org.uk/for-organisations/data-protection-and-brexit/information-rights-and-brexit-frequently-asked-questions/.

Information Integrity Solutions. *Towards a Truly Global Framework for Personal Information Transfers. Comparison and Assessment of EU BCR and APEC CBPR Systems*, 2013. Accessed July 27, 2019. https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f628a8a65e232a6959b80/1465868951114/IIS+CBPR-BCR+report+FINAL.pdf.

Information Technology Industry Council. *ITI Forced Localization Strategy Briefs*, 2016. Accessed January 18, 2018. https://www.itic.org/public-policy/ITIForcedLocalizationStrategyBriefs.pdf.

Insurance Europe. *Comments on the EDPB Guidelines on the GDPR Territorial Scope*, 2019. Accessed May 3, 2019. https://www.insuranceeurope.eu/sites/default/files/attachments/Comments%20on%20the%20EDPB%20guidelines%20on%20the%20GDPR%20territorial%20scope.pdf.

Intel Corporation. *Response to European Commission Public Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009. Accessed August 12, 2019. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/intel_corporation_en.pdf.

International Association of Privacy Professionals, and Ernst & Young. *Annual Privacy Governance Report 2019*, 2019. Accessed January 2, 2020. https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.

International Law Commission. *Report on the Work of Its Fifty- Eighth Session*. UN Doc. A/61/10, 2006. Accessed January 2, 2019. https://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf.

Jääskinen, Niilo, and Angela Ward. "The External Reach of EU Private Law in the Light of L'Oréal versus EBay and Google and Google Spain." In *Private Law in the External Relations of the EU*, edited by Marise Cremona and Hans-W Micklitz, 125–146. 1st ed. Oxford: Oxford University Press, 2016.

Jensen, Eric Talbot. "Cyber Sovereignty: The Way Ahead." *Texas International Law Journal* 50, no. 2 (2015): 275–304. Accessed February 11, 2019. https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1239&context=faculty_scholarship.

Jeong, Sarah. "Zuckerberg Says Facebook Will Extend European Data Protections Worldwide — Kind Of." *The Verge*. Last modified April 11, 2018. Accessed May 28, 2019. https://www.theverge.com/2018/4/11/17224492/zuckerberg-facebook-congress-gdpr-data-protection.

Johnson, David R., and David Post. "Law And Borders – the Rise of Law in Cyberspace." *Stanford Law Review* 48, no. 5 (1996): 1367–1402. Accessed January 31, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535.

Joneja, Navneet. "Google Storage for Developers Open to All, with New Features." *Google Developers Blog*, May 10, 2011. Accessed January 19, 2018. https://developers.googleblog.com/2011/05/google-storage-for-developers-open-to.html.

Jos, Dumortier. “How the Adequacy Mechanism Works: Progress in the EU’s Governance of Cross-Border Data Flows?” Presented at the Computers, Privacy and Data Protection conference, Brussels, January 30, 2019.

Jourová, Věra. *How Will the EU’s Reform Adapt Data Protection Rules to New Technological Developments? - European Commission Factsheet*, 2016. Accessed December 29, 2019. https://op.europa.eu/en/publication-detail/-/publication/2b2f7f00-f5b8-11e7-b8f5-01aa75ed71a1/language-en.

Kamara, Irene, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, and Gabriela Bodea. *Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679*. Brussels: European Commission - DG Justice & Consumers, 2019. Accessed May 1, 2019. https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_final.pdf.

Kamarinou, Dimitra, Christopher Millard, and Isabella Oldani. *Compliance as a Service*. Queen Mary School of Law Legal Studies Research Paper No. 287/2018, 2018. Accessed April 25, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3284497.

Keele, Benjamin J. “Privacy by Deletion: The Need for a Global Data Deletion Principle.” *Indiana Journal of Global Legal Studies* 16, no. 1 (2009): 363–384.

Kent, Gail. “Sharing Investigation Specific Data with Law Enforcement - An International Approach.” *Stanford Public Law Working Paper* (February 14, 2014). Accessed January 23, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413.

King, Kevin F. “Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies.” *Albany Law Journal of Science & Technology* 21 (2011): 61–124.

Kirby, Michael D. “Transborder Data Flows and the ‘Basic Rules’ of Data Privacy.” *Stanford Journal of International Law* 16, no. 2 (1980): 27–66.

Kloza, Dariusz, and Anna Mościbroda. “Making the Case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insights from Competition Law.” *International Data Privacy Law* 4, no. 2 (May 1, 2014): 120–138.

Koops, Bert-Jaap, and Morag Goodwin. *Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law*. Tilburg Law School Legal Studies Research Paper Series No. 05/2016, 2014. Accessed January 23, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263.

KPMG. *Cloud Monitor 2015 Cloud Computing in Germany. Status Quo and Perspectives*, 2015.

Kuner, Christopher. “An International Legal Framework for Data Protection: Issues and Prospects.” *Computer Law & Security Review* 25, no. 4 (2009): 307–317.

———. “Data Nationalism and Its Discontents.” *Emory Law Journal* 64 (2015): 2089–2098. Accessed January 8, 2018. http://law.emory.edu/elj/_documents/volumes/64/online/kuner.pdf.

———. “Data Protection Law and International Jurisdiction on the Internet (Part 2).” *International Journal of Law and Information Technology* 18, no. 3 (2010): 227–247.

———. “Data Protection Law and International Jurisdiction on the Internet (Part I).” *International Journal of Law and Information Technology* 18 (2010): 176–193.

———. “Developing an Adequate Legal Framework for International Data Transfers” (2009). Accessed August 21, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1464323.

———. “Developing an Adequate Legal Framework for International Data Transfers.” In *Reinventing Data Protection*, edited by Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne, and Sjaak Nouwt, 263–273. Springer Netherlands, 2009. Accessed December 8, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1464323&download=yes.

———. *European Data Privacy Law and Online Business*. New York; Oxford: Oxford University Press, 2003.

———. *European Data Protection Law: Corporate Compliance and Regulation*. 2nd ed. New York; Oxford: Oxford University Press, 2007.

———. “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law.” *International Data Privacy Law* 5, no. 4 (2015): 235–245.

———. “Reality and Illusion in EU Data Transfer Regulation Post Schrems.” *German Law Journal* 18, no. 4 (2017): 881–918.

———. *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*. TILT Law & Technology Working Paper No. 016/2010 - Tilburg Law School Research Paper No. 016/2010, 2010. Accessed February 9, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483.

———. *The Internet and the Global Reach of EU Law*. LSE Law, Society and Economy Working Papers 4/2017 - University of Cambridge Faculty of Law Research Paper No. 24/2017, 2017. Accessed June 6, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890930.

Kuner, Christopher, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, and Orla Lynskey. “Internet Balkanization Gathers Pace: Is Privacy the Real Driver?” *International Data Privacy Law* 5, no. 1 (February 1, 2015): 1–2. Accessed January 30, 2018. http://dx.doi.org/10.1093/idpl/ipu032.

Lecher, Colin. “Democratic Senators Have Introduced a Big New Data Privacy Plan.” *The Verge*. Last modified December 12, 2018. Accessed May 25, 2019. https://www.theverge.com/2018/12/12/18138131/democratic-data-care-act-senate-law.

———. “Sen. Ron Wyden Proposes Bill That Could Jail Executives Who Mishandle Consumer Data.” *The Verge*. Last modified November 1, 2018. Accessed May 25, 2019. https://www.theverge.com/2018/11/1/18052254/ron-wyden-privacy-bill-draft-consumer-tracking.

Lee, Amanda. “US to Appoint Permanent Privacy Shield Ombudsperson, as EU Pressure Tells.” *Euractiv.Com*, January 23, 2019. Accessed April 27, 2019. https://www.euractiv.com/section/data-protection/news/us-to-appoint-permanent-privacy-shield-ombudsperson-following-eu-pressure/.

Lee, Stacia. “International Reactions to U.S. Cybersecurity Policy: The BRICS Undersea Cable.” *The Henry M. Jackson School of International Studies*, January 8, 2016. Accessed October 27, 2019. https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/.

Leite Monteiro, Renato. “Changes to Brazil’s Data Protection Law and the Establishment of the DPA.” *Iapp*, January 3, 2019. Accessed May 24, 2019. https://iapp.org/news/a/changes-to-brazils-data-protection-law-and-the-establishment-of-the-dpa/.

———. “The New Brazilian General Data Protection Law — a Detailed Analysis.” *Iapp*, August 15, 2018. Accessed May 24, 2019. https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/.

Leviathan Security Group. *Analysis of Cloud vs. Local Storage: Capabilities, Opportunities, Challenges*, 2015. Accessed January 20, 2018. https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dada7e4b069728afca39b/1436396967533/Value+of+Cloud+Security+-+Scarcity.pdf.

———. *Comparison of Availability Between Local and Cloud Storage*, 2015. Accessed January 22, 2018. https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad9ae4b069728afca34a/1436396954508/Value+of+Cloud+Security+-+Availability.pdf.

———. *Quantifying the Cost of Forced Localization*, 2015. Accessed January 24, 2018. https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

Lindqvist, Jenna. "New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?" *International Journal of Law and Information Technology* 26, no. 1 (2018): 45–63.

Linklaters. *A Framework Fit for the Twenty-First Century. A Response to the Commission's Public Consultation*, 2009. Accessed August 12, 2019. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/unregistered_organisations/linklaters_llp_en.pdf.

———. "The European Court of Justice to Rule on the Validity of Standard Contractual Clauses." Last modified June 1, 2016. Accessed August 6, 2018. https://www.linklaters.com/en/insights/publications/2016/june/the-european-court-of-justice-to-rule-on-the-validity-of-standard-contractual-clauses.

Linn, Emily. "A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement Notes." *Vanderbilt Journal of Transnational Law* 50 (2017): 1311–1358.

Lumb, David. "Why Apple Is Spending $1.9 Billion To Open Data Centers In Denmark And Ireland." *Fast Company*. Last modified February 23, 2015. Accessed January 20, 2018. https://www.fastcompany.com/3042746/why-apple-is-spending-19-billion-to-open-data-centers-in-denmark-and-ireland.

Madge, Robert. "GDPR's Global Scope: The Long Story." *MyData Journal*, May 12, 2018. Accessed April 12, 2019. https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f.

Mantelero, Alessandro. "Cloud Computing, Trans-Border Data Flows and the European Directive 95/46/EC: Applicable Law and Task Distribution." *European Journal of Law and Technology* 3, no. 2 (n.d.): 1–6.

———. "I Flussi Di Dati Transfrontalieri e Le Scelte Delle Imprese Tra Safe Harbour e Privacy Shield." In *La Protezione Transnazionale Dei Dati Personali. Dai "Safe Harbour Principles" al "Privacy Shield,"* edited by Giorgio Resta and Vincenzo Zeno-Zencovich, 239 – 269. Roma: Roma Tre-press, 2016.

———. "Il Futuro Regolamento EU Sui Dati Personali e La Valenza 'Politica' Del Caso Google: Ricordare e Dimenticare Nella Digital Economy." *Il Diritto dell'Informazione e dell'Informatica*, no. 4–5 (2014): 681 – 701.

Mari, Angelica. "Brazil Moves Forward with Online Data Protection Efforts." *ZDNet*. Last modified July 5, 2018. Accessed August 3, 2018. https://www.zdnet.com/article/brazil-moves-forward-with-online-data-protection-efforts/.

Markoff, John. "Microsoft Plumbs Ocean's Depths to Test Underwater Data Center." *The New York Times*, January 31, 2016. Accessed April 7, 2018. https://www.nytimes.com/2016/02/01/technology/microsoft-plumbs-oceans-depths-to-test-underwater-data-center.html.

McCusker, Shona. "The EU-US Privacy Shield: The Antidote to the Transatlantic Data Transfer Headache?" *Business Law Review* 37, no. 3 (2016): 84–85.

McNabb, Nathalie, and Soeren Klaebel Clemmensen. “GDPR Update: The Future of International Data Transfers.” *Deloitte*. Accessed January 17, 2019. https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-future-of-international-data-transfers.html.

McQuinn, Alan, and Daniel Castro. *How Law Enforcement Should Access Data Across Borders*. Information Technology and Innovation Foundation, 2017. Accessed January 23, 2018. http://www2.itif.org/2017-law-enforcement-data-borders.pdf.

Meltzer, Joshua. *Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium Sized Enterprises and Developing Countries*. Global Economy and Development Working Paper 69, The Brookings Institution, 2014. Accessed January 24, 2018. https://www.brookings.edu/wp-content/uploads/2016/07/02-internet-international-trade-meltzer.pdf.

———. *The Internet, Cross-Border Data Flows and International Trade*. Issues in Technology Innovation, Center for Technology Innovation at Brookings, 2013. Accessed November 2, 2019. https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf.

Menthe, Darrel C. “Jurisdiction in Cyberspace: A Theory of International Spaces.” *Michigan Telecommunications and Technology Law Review* 4, no. 1 (1998): 69 – 103. Accessed January 31, 2018. https://repository.law.umich.edu/cgi/viewcontent.cgi?referer=https://www.google.co.uk/&httpsredir=1&article=1163&context=mttlr.

Microsoft Corporation. *Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009. Accessed August 6, 2018. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/microsoft_corporation_en.pdf.

Millard, Christopher. “Forced Localization of Cloud Services: Is Privacy the Real Driver?” *IEEE Cloud Computing* 2, no. 2 (April 2015): 10–14.

———. *Legal Protection of Computer Programs and Data*. London: Sweet & Maxwell, 1985.

Miller, Claire Cain. “Revelations of N.S.A. Spying Cost U.S. Tech Companies.” *The New York Times*, March 21, 2014. Accessed January 20, 2018. https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

Miller, John, and Sana Ali. “No Safety in Silos.” *Information Technology Industry Council*. Last modified August 16, 2016. Accessed February 19, 2018. http://www.itic.org/news-events/techwonk-blog/no-safety-in-silos?

Miller, Rich. “Google Gets Patent for Data Center Barges.” *Data Center Knowledge*. Last modified April 29, 2009. Accessed April 7, 2018. http://www.datacenterknowledge.com/archives/2009/04/29/google-gets-patent-for-data-center-barges.

Moerel, Lokke. “Back to Basics: When Does EU Data Protection Law Apply?” *International Data Privacy Law* 1, no. 2 (2011): 92–110.

———. *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*. Oxford: Oxford University Press, 2012.

———. “GDPR Conundrums: Data Transfer,” June 9, 2016. Accessed August 7, 2018. https://iapp.org/news/a/gdpr-conundrums-data-transfer/.

———. “GDPR Conundrums: The GDPR Applicability Regime — Part 1: Controllers,” January 29, 2018. Accessed April 13, 2018. https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/.

———. “GDPR Conundrums: The GDPR Applicability Regime — Part 2: Processors,” February 6, 2018. Accessed April 10, 2018. https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-2-processors/.

———. “The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?” *International Data Privacy Law* 1, no. 1 (2011): 28–46.

Mole, Ariane, Ruth Boardman, Gabe Maldoff, and Gabriel Voisin. “Where Does the GDPR Apply? European Data Protection Board Finally Weighs In.” *Bird & Bird*. Last modified November 2018. Accessed May 3, 2019. http://www.twobirds.com/en/news/articles/2018/global/where-does-the-gdpr-apply-european-data-protection-board-finally-weighs-in.

Monteleone, Shara, and Laura Puccio. *From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules*. European Parliamentary Research Service, 2017. Accessed August 2, 2018. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf.

Monti, Giorgio. “The Global Reach of EU Competition Law.” In *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, edited by Marise Cremona and Joanne Scott. 1st ed. Oxford: Oxford University Press, 2019.

Movius, Lauren B., and Nathalie Krup. “U.S. and EU Privacy Policy: Comparison of Regulatory Approaches.” *International Journal of Communication* 3 (2009): 169–187. Accessed February 7, 2018. http://ijoc.org/index.php/ijoc/article/view/405/305.

Nicholson, Jessica R., and Ryan Noonan. *Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services*. ESA Issue Brief # 01-14, United States Department of Commerce: Economics and Statistics Administration, 2014. Accessed January 25, 2018. https://www.tralac.org/images/News/Documents/Digital_Economy_and_Cross-Border_Trade_ESA_Issue_Brief_January_2014_US_Department_of_Commerce.pdf.

Nielsen, Nikolaj. “Privacy Shield Less Relevant given GDPR, Says Data Chief.” *EUobserver*, May 24, 2018. Accessed May 26, 2018. https://euobserver.com/justice/141886.

Novotny, Eric J. “Transborder Data Flows and International Law: A Framework for Policy-Oriented Inquiry.” *Stanford Journal of International Law* 16, no. 2 (1980): 141–180.

NTT Communications. *NSA After-Shocks. How Snowden Has Changed ICT Decision-Makers’ Approach to the Cloud*, 2014. Accessed January 20, 2018. http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf.

Nugraha, Yudhistira, Kautsarina, and Ashwin Sastrosubroto. “Towards Data Sovereignty in Cyberspace” Presented at the Third International Conference of Information and Communication Technology, Bali, Indonesia, May 2015. Accessed February 15, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2610314.

Office of the Privacy Commissioner of Canada. “Announcement: Commissioner Concludes Consultation on Transfers for Processing.” Last modified September 23, 2019. Accessed December 24, 2019. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/.

———. “Consultation on Transborder Dataflows.” Last modified June 11, 2019. Accessed August 31, 2019. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/.

———. “Consultation on Transfers for Processing – Reframed Discussion Document.” Last modified June 11, 2019. Accessed August 31, 2019. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/#fn6-rf.

———. “Getting Accountability Right with a Privacy Management Program.” Last modified April 17, 2012. Accessed August 31, 2019. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/.

———. *PIPEDA – Processing Personal Data Across Borders Guidelines*, 2009. Accessed August 2, 2019. https://www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf.

———. “Supplementary Discussion Document – Consultation on Transborder Dataflows.” Last modified June 11, 2019. Accessed August 31, 2019. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/sup_tbdf_201904/.

Olson, Jeff, and Mai Phuong Nguyen. “Vietnam Quick to Enforce New Cybersecurity Law.” *HL Chronicle of Data Protection*. Last modified March 6, 2019. Accessed October 27, 2019. https://www.hldataprotection.com/2019/03/articles/international-eu-privacy/vietnam-quick-to-enforce-new-cybersecurity-law/.

Olson, Jeff, Eddie O’shea, and Mai Phuong Nguyen. “Update: Vietnam’s New Cybersecurity Law.” *HL Chronicle of Data Protection*. Last modified November 15, 2018. Accessed October 27, 2019. https://www.hldataprotection.com/2018/11/articles/international-eu-privacy/update-vietnams-new-cybersecurity-law/.

Orange/France Telecom Group. *Contribution to the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009. Accessed August 6, 2018. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/orange_en.pdf.

Organisation for Economic Cooperation and Development. *Economic and Social Benefits of Internet Openness*. Paris: OECD Digital Economy Papers No. 257, OECD Publishing, 2016. Accessed February 16, 2018. http://www.oecd-ilibrary.org/docserver/download/5jlwqf2r97g5-en.pdf?expires=1519237452&id=id&accname=guest&checksum=F97665039CC2F5EC59376BE4F8E314D7.

———. *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. C(80)58/FINAL, 1980.

———. *Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy*, 2007. Accessed April 15, 2019. http://www.oecd.org/internet/ieconomy/38770483.pdf.

———. *Report on Compliance with, and Enforcement of, Privacy Protection Online*, 2003. Accessed August 24, 2019. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2002)5/FINAL&docLanguage=En.

———. *Report on the Cross-Border Enforcement of Privacy Laws*, 2006. Accessed April 14, 2019. http://www.oecd.org/internet/ieconomy/37558845.pdf.

———. *The OECD Privacy Framework*, 2013. Accessed May 22, 2019. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Osula, Anna-Maria. “Transborder Access and Territorial Sovereignty.” *Computer Law & Security Review* 31 (2015): 719–735.

Özer, Yusuf Mansur. “GDPR Matchup: Turkey’s Data Protection Law,” August 10, 2017. Accessed October 27, 2019. https://iapp.org/news/a/gdpr-matchup-turkeys-data-protection-law/.

Palazzi, Pablo A., and Andres Chomczyk. “GDPR Matchup: Argentina’s Draft Data Protection Act.” *Iapp*, August 24, 2017. Accessed May 29, 2019. https://iapp.org/news/a/gdpr-matchup-argentinas-draft-data-protection-act/.

Palmer, Michael. “Data Is the New Oil.” *ANA Marketing Maestros*. Last modified November 3, 2006. Accessed February 16, 2018. http://ana.blogs.com/maestros/2006/11/data_is_the_new.html.

Panetta, Leon E. “Remarks on Cybersecurity to the Business Executives for National Security,” New York City, October 11, 2012. Accessed January 25, 2018. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Pegoraro, Rob. “Why 2019 Might Finally Bring a National Privacy Law for the US.” *Yahoo! Finance*. Last modified December 31, 2018. Accessed May 25, 2019. https://finance.yahoo.com/news/why-2019-might-finally-bring-144821100.html.

Personal Investment Management & Financial Advice Association. *Response to the EDPB Consultation on Guidelines 3/2018 on the Territorial Scope of the GDPR*, 2019. Accessed May 2, 2019. https://www.pimfa.co.uk/wp-content/uploads/2019/01/PIMFA-response-to-EDPB-cp-on-guidelines-on-territorial-scope.pdf.

PHAEDRA. *Co-Ordination and Co-Operation between Data Protection Authorities*, 2014. Accessed April 15, 2019. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf.

Piroddi, Paola. “I Trasferimenti Di Dati Personali Verso Paesi Terzi Dopo La Sentenza Schrems e Nel Nuovo Regolamento Generale Sulla Protezione Dei Dati.” In *La Protezione Transnazionale Dei Dati Personali. Dai “Safe Harbour Principles” al “Privacy Shield,”* edited by Giorgio Resta and Vincenzo Zeno-Zencovich, 169 – 213. Roma: Roma Tre-press, 2016.

Poullet, Yves, Sophie Louveaux, and Maria Veronia Perez Asinari. “Data Protection and Privacy in Global Networks: A European Approach.” *The EDI Law Review* 8 (2001): 147–196.

Practice. *Risk-Aware Deployment and Intermediate Report on Status of Legislative Developments in Data Protection*, 2015. Accessed April 10, 2018. https://practice-project.eu/downloads/publications/Deliverables-Y2/D31.2-Risk-aware-deployment-PU-M24.pdf.

Prete, Luca. “On Implementation and Effects: The Recent Case-Law on the Territorial (or Extraterritorial?) Application of EU Competition Rules.” *Journal of European Competition Law & Practice* 9, no. 8 (October 1, 2018): 487–495.

Pringle, Ramona. “‘Data Is the New Oil’: Your Personal Information Is Now the World’s Most Valuable Commodity.” *CBC News*. Last modified August 25, 2017. Accessed December 31, 2017. http://www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677.

Prins, Corien. “Should ICT Regulation Be Undertaken at an International Level?” In *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, edited by Bert-Jaap Koops, Corien Prins, Maurice Schellekens, and Miriam Lips, 151–201. T.M.C. Asser Press, 2006.

Proust, Olivier, and Emmanuelle Bartoli. “Binding Corporate Rules: A Global Solution for International Data Transfers.” *International Data Privacy Law* 2, no. 1 (2012): 35–39.

Rabben, Roland. “It’s Your Stuff — Guaranteed!” *Jottacloud*. Last modified June 16, 2013. Accessed January 20, 2018. https://blog.jottacloud.com/its-your-stuff-guaranteed-3f50359f72d.

Rackspace. *Consultation Paper on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 2009. Accessed July 31, 2018. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/unregistered_organisations/rackspace_us_inc_en.pdf.

Ramey, Melanie. “Brazil’s New General Data Privacy Law Follows GDPR Provisions.” *Inside Privacy*. Last modified August 20, 2018. Accessed May 24, 2019. https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/.

Reed, Chris. “Cloud Governance: The Way Forward.” In *Cloud Computing Law*, 362–389. Oxford: Oxford University Press, 2013.

Reidenberg, Joel R. “Resolving Conflicting International Data Privacy Rules in Cyberspace.” *Stanford Law Review* 52, no. 5 (2000): 1315 – 1371. Accessed February 7, 2018. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1040&context=faculty_scholarship.

Riccio, Giovanni Maria. “Model Contract Clauses e Corporate Binding Rules: Valide Alternative al Safe Harbor Agreement?” In *La Protezione Transnazionale Dei Dati Personali. Dai “Safe Harbour Principles” al “Privacy Shield,”* edited by Giorgio Resta and Vincenzo Zeno-Zencovich, 215 – 238. Roma: Roma Tre-press, 2016.

Ridout, T. A. “Marco Civil: Brazil’s Push to Govern the Internet.” *Huffington Post*, October 22, 2013. Accessed January 26, 2018. https://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html.

Roach, John. “Under the Sea, Microsoft Tests a Datacenter That’s Quick to Deploy, Could Provide Internet Connectivity for Years.” *Microsoft*. Last modified June 5, 2018. Accessed November 24, 2019. https://news.microsoft.com/features/under-the-sea-microsoft-tests-a-datacenter-thats-quick-to-deploy-could-provide-internet-connectivity-for-years/.

Roberts, Paul. “Interdisciplinarity in Legal Research.” In *Research Methods for Law*, edited by Michael McConville and Chui, 90–133. Second edition. Edinburgh: Edinburgh University Press, 2017.

Ronco, Emmanuel, and Natalie Farmer. “EDPB Issues First Opinion on Administrative Arrangements Under the GDPR for Cross-Border Data Flows Between EU and Non-EU Securities Agencies.” *Cleary Cybersecurity and Privacy Watch*. Last modified March 15, 2019. Accessed May 1, 2019. https://www.clearycyberwatch.com/2019/03/edpb-issues-first-opinion-on-administrative-arrangements-under-the-gdpr-for-cross-border-data-flows-between-eu-and-non-eu-securities-agencies/.

Rosenwald, Michael S. “Cloud Centers Bring High-Tech Flash but Not Many Jobs to Beaten-down Towns.” *The Washington Post*, November 24, 2011. Accessed January 22, 2017. https://www.washingtonpost.com/business/economy/cloud-centers-bring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html?utm_term=.6b1093c1893c.

Rossi, Agustín. “Internet Privacy: Who Sets the Global Standard?” *The International Spectator* 49, no. 1 (2014): 65–80.

Rugani, Gabriele. “Data Protection Provisions in New Generation Free Trade Agreements: Advantages and Critical Issues.” In *“The New Generation of EU FTAs: External and Internal Challenges,”* edited by Isabelle Bosse-Platière, Cécile Rapoport, and Nicolas Pigeon, 60–74. LAwTTIP Working Papers 2019/6, 2019. Accessed July 1, 2020. https://www.lawttip.eu/uploads/files/LAwTTIP%20Working%20Paper_2019_6_Event%2013(1).pdf.

Ruiz, David. “Responsibility Deflected, the CLOUD Act Passes.” *Electronic Frontier Foundation*. Last modified March 22, 2018. Accessed May 6, 2019. https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes.

Ryngaert, Cedric. *Jurisdiction in International Law*. Second ed. Oxford, United Kingdom; New York, NY: Oxford University Press, 2015.

Sachdeva, Amit M. “International Jurisdiction in Cyberspace: A Comparative Perspective.” *Computer and Telecommunications Law Review* 13, no. 8 (2007): 245–258.

Salgado, Richard. “Written Testimony before the Senate Judiciary Subcommittee on Privacy, Technology and the Law” Presented at the Hearing on “The Surveillance Transparency Act of 2013,” November 13, 2013. Accessed January 20, 2018. http://services.google.com/fh/files/blogs/google_testimony_transparency_nov132013.pdf.

Saraf, Bharat, and Ashraf U. Sarah Sarah Kazi. “Analysing the Application of Brussels I in Regulating E-Commerce Jurisdiction in the European Union – Success, Deficiencies and Proposed Changes.” *Computer Law & Security Review* 29, no. 2 (2013): 127–143.

Sartor, Giovanni, and Mario Viola de Azevedo Cunha. “Il Caso Google e i Rapporti Regolatori USA/EU.” *Il Diritto dell’Informazione e dell’Informatica*, no. 4–5 (2014): 657–680.

Sauer, Ralf. “How the Adequacy Mechanism Works: Progress in the EU’s Governance of Cross-Border Data Flows?” Presented at the Computers, Privacy and Data Protection conference, Brussels, January 30, 2019.

Schmitt (ed), Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. Accessed January 30, 2018. https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

Scott, Mark, and Nick Wingfield. “Microsoft Suggests Wider Options for Foreign Data.” *Bits Blog, The New York Times*, January 23, 2014. Accessed January 20, 2018. https://bits.blogs.nytimes.com/2014/01/23/microsoft-suggests-wider-options-for-foreign-data/?mtrref=www.google.co.uk&gwh=8445EBC1CBAF8943DD76801BB17A3EE7&gwt=pay.

Selby, John. “Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?” *International Journal of Law and Information Technology* 25, no. 3 (2017): 213–232.

Senz, Deborah, and Hilary Charlesworth. “Building Blocks: Australia’s Response to Foreign Extraterritorial Legislation.” *Melbourne Journal of International Law* 2, no. 1 (2001): 69–121.

Sica, Salvatore, and Virgilio D’Antonio. “Verso Il Privacy Shield: Il Tramonto Dei Safe Harbour Privacy Principles.” In *La Protezione Transnazionale Dei Dati Personali. Dai “Safe Harbour Principles” al “Privacy Shield,”* edited by Giorgio Resta and Vincenzo Zeno-Zencovich, 137 – 167. Roma: Roma Tre-press, 2016.

Silverstone, Ariel, John Wunderlich, Sholem Prasow, and Stephan Grynwajc. “European Parliament Voted to Suspend Privacy Shield: Now What?” *Iapp*, September 25, 2018. Accessed January 14, 2019. https://iapp.org/news/a/european-parliament-voted-to-suspend-privacy-shield-now-what/.

Smith, Brad. *Statement of 21 March 2018 on the Inclusion of the CLOUD Act in the Omnibus Funding Bill*, 2018. Accessed May 6, 2019. https://perma.cc/QKN2-H5W5.

———. “The Need for a Digital Geneva Convention” Presented at the RSA Conference, San Francisco, California, February 14, 2017. Accessed February 9, 2018. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Smith, David. “ICO Brings Some Welcome Clarification to the GDPR’s International Transfer Rules.” *Allen & Overy - Digital Hub*, September 7, 2018. Accessed February 10, 2019. http://aodigitalhub.com/2018/09/07/ico-brings-some-welcome-clarification-to-the-gdprs-international-transfer-rules/.

Solove, Daniel. “Beyond GDPR: The Challenge of Global Privacy Compliance - An Interview with Lothar Determann.” *PRIVACY + SECURITY BLOG*, November 13, 2017. Accessed May 27, 2019. https://teachprivacy.com/challenge-of-global-privacy-compliance/.

Stegmaier, Gerard, and Ariana Goodell. “Facebook Announces Plan to Implement GDPR Globally.” *ReedSmith - Technology Law Dispatch*. Last modified April 9, 2018. Accessed May 28, 2019. https://www.technologylawdispatch.com/2018/04/privacy-data-protection/facebook-announces-plan-to-implement-gdpr-globally/.

Sullivan, Clare. “EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era.” *Computer Law & Security Review* 35, no. 4 (2019): 380–397.

Suwanprateep, Dhiraphol. “Get Ready: The First Thailand Personal Data Protection Act Has Been Passed.” *Baker McKenzie*. Last modified March 1, 2019. Accessed June 5, 2019. https://www.bakermckenzie.com/en/insight/publications/2019/03/the-first-thailand-personal-data.

Suwanprateep, Dhiraphol, and Nont Horayangura. “Thailand Personal Data Protection Act.” *Baker McKenzie*. Last modified May 28, 2019. Accessed June 5, 2019. https://www.bakermckenzie.com/en/insight/publications/2019/05/thailand-personal-data-protection-act.

Svantesson, Dan Jerker B. “Delineating the Reach of Internet Intermediaries’ Content Blocking - CcTLD Blocking, Strict Geo-Location Blocking or a Country Lens Approach.” *SCRIPTed: A Journal of Law, Technology and Society* 11 (2014): 153–170.

———. “Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation.” *International Data Privacy Law* 5, no. 4 (2015): 226–234.

———. *Extraterritoriality in Data Privacy Law*. Copenhagen: Ex Tuto Publishing, 2013.

———. “Geo-Location Technologies and Other Means of Placing Borders on the ‘Borderless’ Internet.” *The John Marshall Journal of Computer and Information Law* 23, no. 1 (2004): 101–139.

———. “Pammer and Hotel Alpenhof – ECJ Decision Creates Further Uncertainty about When e-Businesses ‘Direct Activities’ to a Consumer’s State under the Brussels I Regulation.” *Computer Law & Security Review* 27, no. 3 (2011): 298–304.

———. “The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses.” *Stanford Journal of International Law* 50, no. 1 (2014): 53–102.

———. “Time for the Law to Take Internet Geolocation Technologies Seriously.” *Journal of private international law* 8, no. 3 (2012): 473–487.

Svantesson, Dan Jerker B., and Felicity Q.C. Gerry. “Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond.” *Computer Law & Security Review* 31 (2015): 478–489.

Sverdlik, Yevgeniy. “Microsoft Wants to Patent an Underwater Data Center.” *Data Center Knowledge*. Last modified January 9, 2017. Accessed April 7, 2018. http://www.datacenterknowledge.com/archives/2017/01/09/microsoft-wants-to-patent-an-underwater-data-center-reef.

Taylor, Mistale. “The EU’s Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect.” *International Data Privacy Law* 5, no. 4 (November 1, 2015): 246–256.

de Terwangne, Cécile. “Is a Global Data Protection Regulatory Model Possible?” In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cecile De Terwangne, and Sjaak Nouwt, 175–189. Amsterdam: Springer, 2009.

The Business Roundtable. *Putting Data to Work: Maximizing the Value of Information in an Interconnected World*, 2015. Accessed February 7, 2018. http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf.

The European Consumer Organization (BEUC) - Press Release. “Privacy Shield Opens Hole in Protection of EU Citizens’ Privacy.” Last modified July 12, 2016. Accessed August 3, 2018. https://www.beuc.eu/publications/beuc-pr-2016-011_privacy_shield_-_adequacy_agreement.pdf.

Thomas, Thomas K. “Indian Net Firms Want Google, Facebook to Go ‘Local.’” *The Hindu Business Line*. Last modified June 8, 2013. Accessed January 22, 2018. http://www.thehindubusinessline.com/info-tech/indian-net-firms-want-google-facebook-to-go-local/article4795367.ece.

Toonders, Joris. “Data Is the New Oil of the Digital Economy.” *WIRED*. Accessed December 31, 2017. https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/.

de la Torre, Lydia. “GDPR Matchup: The California Consumer Privacy Act 2018.” *Iapp*, July 31, 2018. Accessed May 26, 2019. https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/.

Tracol, Xavier. “EU–U.S. Privacy Shield: The Saga Continues.” *Computer Law & Security Review* 32, no. 5 (October 1, 2016): 775–777.

Turn, Rein. “An Overview of Transborder Data Flow Issues” Presented at the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1980. Accessed February 7, 2018. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6233696.

United Nations Conference on Trade and Development. *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 2016. Accessed August 3, 2018. http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

United Nations General Assembly. *Guidelines for the Regulation of Computerized Personal Data Files*, 1990.

———. *International Covenant on Civil and Political Rights*, 1966.

———. *Report of the International Law Commission Fifty-Eighth Session (1 May-9 June and 3 July-11 August 2006*. A/61/10, 2006.

———. *Report of the Special Rapporteur on the Right to Privacy*. A/73/45712, 2018.

———. *Resolution on the Right to Privacy in the Digital Age*. A/RES/68/167, 2013.

———. *Revised Draft Resolution on the Right to Privacy in the Digital Age*. A/C.3/69/L.26/Rev.1, 2014.

———. *Revised Draft Resolution on the Right to Privacy in the Digital Age*. A/C.3/71/L.39/Rev.1, 2016.

———. *Universal Declaration of Human Rights*, 1948.

United Nations Human Rights Council. *The Promotion, Protection and Enjoyment of Human Rights on the Internet, 32nd Session*. A/HRC/32/L.20, 2016. Accessed January 2, 2019. https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

———. *The Right to Privacy in the Digital Age*. A/HRC/28/L.27, 2015.

———. *The Right to Privacy in the Digital Age*. A/HRC/34/L.7/Rev.1, 2017.

United Nations Office on Drugs and Crime. *Comprehensive Study on Cybercrime*, 2013. Accessed January 23, 2018. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

United States Government. *Brief in Support of the Magistrate Judge’s Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within Its Custody and Control, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*. 1:13-mj-

02814, 2014. Accessed January 23, 2018. https://blogs.microsoft.com/wp-content/uploads/sites/149/2017/02/the-government-brief.pdf.

United States Government Accountability Office. *Report to the Chairman, Committee on Energy and Commerce, House of Representatives. INTERNET PRIVACY - Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, 2019. Accessed May 24, 2019. https://assets.documentcloud.org/documents/5736212/GAO-privacy-report.pdf.

US Chamber of Commerce, and Hunton & Williams. *Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity*, 2014. Accessed August 7, 2018. https://www.uschamber.com/sites/default/files/documents/files/021384_BusinessWOBorders_final.pdf.

U.S. Department of Justice. *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, 2019. Accessed May 6, 2019. https://www.justice.gov/dag/page/file/1153436/download.

Ustaran, Eduardo. "EDPB's Common Sense Approach to the GDPR's Territorial Scope." *Iapp*, November 26, 2018. Accessed February 7, 2019. https://iapp.org/news/a/edpbs-common-sense-approach-to-the-gdprs-territorial-scope/.

Vasquez Callo-Müller, María. *GDPR and CBPR: Reconciling Personal Data Protection and Trade*. APEC Policy Support Unit - Policy Brief No. 23, 2018. Accessed August 19, 2019. https://www.apec.org/Publications/2018/10/GDPR-and-CBPR---Reconciling-Personal-Data-Protection-and-Trade.

Velli, Federica. "European Papers." *The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements* 4, no. 3 (2019): 881–894. Accessed July 1, 2020. http://www.europeanpapers.eu/en/europeanforum/issue-of-data-protection-in-eu-trade-commitments.

Vincent, James. "UN Condemns Internet Access Disruption as a Human Rights Violation." *The Verge*. Last modified July 4, 2016. Accessed January 26, 2018. https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access.

Voss, W. Gregory. "The Future of Transatlantic Data Flows: Privacy Shield Or Bust?" *Journal of Internet Law* 19, no. 11 (2016): 9–18.

Walden, Ian. "Law Enforcement Access to Data in Clouds." In *Cloud Computing Law*, edited by Christopher Millard, 285–310. Oxford: Oxford University Press, 2013.

Wall, Alex. "GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules." *Iapp*, May 31, 2017. Accessed August 22, 2019. https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/.

Wandall, Hilary, and Daniel Cooper. "How to Align APEC and EU Cross-Border Transfer Rules." *LAW360*, April 12, 2016. Accessed August 20, 2019. https://www.cov.com/-/media/files/corporate/publications/2016/04/how_to_align_apec_and_eu_cross_border_transfer_rules.pdf.

Waters, Nigel. *The APEC Asia-Pacific Privacy Initiative: A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation?* UNSW Law Research Paper No. 2008-59, 2008. Accessed August 22, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1402445.

Watson, Paul Joseph. "BRICS Countries Build New Internet to Avoid NSA Spying." *Infowars*, October 24, 2013. Accessed January 25, 2018. https://www.infowars.com/brics-countries-build-new-internet-to-avoid-nsa-spying/.

White, David, and Tom Morrison. “Mind the GDPR: Processors & Data Processing Agreements.” *New Law Journal* 168, no. 7788 (2018): 12–13.

Wolters, P. T. J. “The Enforcement by the Data Subject Under the GDPR.” *Journal of Internet Law* 22, no. 8 (2019): 22–31.

Woods, Andrew K. *Data Beyond Borders. Mutual Legal Assistance in the Internet Age*. Global Network Initiative, 2015. Accessed January 23, 2018. http://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1517&context=law_facpub.

Working Group on International Enforcement Cooperation. *Final Report - 41st International Conference for Data Protection and Privacy Commissioners*, 2019. Accessed December 22, 2019. https://privacyconference2019.info/wp-content/uploads/2019/11/ICDPPC-WGIEC-Final-Report-October-2019-published-final-1.pdf.

World Trade Organization. *Joint Statement on Electronic Commerce*. WT/L/1056, 2019. Accessed June 5, 2019. http://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf.

———. *Joint Statement on Electronic Commerce. EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce. Communication from the European Union*. INF/ECOM/22, 2019. Accessed June 5, 2019. http://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

Yakovleva, Svetlana, and Kristina Irion. “Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade.” *International Data Privacy Law* (n.d.): 1–21. Accessed June 28, 2020. http://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaa003/5813832.

York, Jillian C. “Is Iran’s Halal Internet Possible?” *Aljazeera*. Last modified October 2, 2012. Accessed January 2, 2018. http://www.aljazeera.com/indepth/opinion/2012/10/201210263735487349.html.

Zeno-Zencovich, Vincenzo. “Intorno Alla Decisione Nel Caso Schrems: La Sovranità Digitale e Il Governo Internazionale Delle Reti Di Telecomunicazione.” In *La Protezione Transnazionale Dei Dati Personali. Dai “Safe Harbour Principles” al “Privacy Shield,”* edited by Giorgio Resta and Vincenzo Zeno-Zencovich, 7 – 22. Roma: Roma Tre-press, 2016.

Zoetekouw, M. “Ignorantia Terrae Non Excusat” Presented at the Crossing Borders: Jurisdiction in Cyberspace Conference, Amsterdam, the Netherlands, March 2016. Accessed November 2, 2019. https://c.ymcdn.com/sites/www.iisfa.net/resource/resmgr/Slide_seminari/Convegno_Milano/c-mzoetekouw-ignorantia-terr.pdf.

Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (2019/C 384 I/01). OJ C 384 I/1, 2019.

“AmCham EU Welcomes Announcement to Nominate Privacy Shield Ombudsperson.” *AmCham EU*. Last modified January 24, 2019. Accessed April 27, 2019. http://www.amchameu.eu/news/amcham-eu-welcomes-announcement-nominate-privacy-shield-ombudsperson.

APEC Cross-Border Privacy Rules System. Policies, Rules and Guidelines, 2019. Accessed August 19, 2019. http://cbprs.org/documents/.

APEC Cross-Border Privacy Rules System Program Requirements, 2019. Accessed August 31, 2019. http://cbprs.org/documents/.

APEC Privacy Framework, 2005. Accessed August 31, 2019. https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

APEC Privacy Framework, 2015. Accessed August 31, 2019. https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

APEC Privacy Recognition for Processors ("PRP"). Purpose and Background, n.d. Accessed August 4, 2019. http://cbprs.org/documents/.

APEC Privacy Recognition for Processors System. Policies, Rules and Guidelines, n.d. Accessed August 4, 2019. http://cbprs.org/documents/.

"Apple to Invest €1.7 Billion in New European Data Centres." *Apple Newsroom*. Last modified February 23, 2015. Accessed January 20, 2018. https://www.apple.com/newsroom/2015/02/23Apple-to-Invest-1-7-Billion-in-New-European-Data-Centres/.

"Argentina Publishes GDPR-Style Data Protection Bill." *Privacy Laws & Business*. Last modified September 24, 2018. Accessed May 29, 2019. https://www.privacylaws.com/news/argentina-publishes-gdpr-style-data-protection-bill/.

"Brazil Plans to Go Offline from US-Centric Internet." *The Hindu*, September 17, 2013. Accessed January 26, 2018. http://www.thehindu.com/news/international/world/brazil-plans-to-go-offline-from-uscentric-internet/article5137689.ece.

"Business Roundtable Releases Framework for National Consumer Privacy Law." *Business Roundtable*. Last modified December 6, 2018. Accessed May 25, 2019. https://www.businessroundtable.org/business-roundtable-releases-framework-for-national-consumer-privacy-law.

Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). S.C. 2000, c. 5, 2000.

Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 23 March 2018. H.R. 4943, 2018.

Coalition Letter from American Civil Liberties Union et al. to US Members of Congress of 12 March 2018, 2018. Accessed May 6, 2019. https://www.aclu.org/sites/default/files/field_document/cloud_act_coalition_letter_3-8_clean.pdf.

Cybersecurity Law of the People's Republic of China, 24th Session of the Standing Committee of the 12th National People's Congress, 2016.

"Data Privacy Law: The Top Global Developments in 2018 and What 2019 May Bring." *DLA Piper*. Last modified February 25, 2019. Accessed June 4, 2019. https://www.dlapiper.com/en/belgium/insights/publications/2019/02/data-privacy-law-2018-2019/.

"Data Privacy Subgroup Meeting with European Union." *Asia-Pacific Economic Cooperation*. Accessed July 30, 2019. https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union.

Decree No. 72/2013/ND-CP on Management, Provision and Use of Internet Services and Online Information, 2013. Accessed February 21, 2018. https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF.

"DPA of Argentina Issues Draft Data Protection Bill." *Privacy & Information Security Law Blog*, February 9, 2017. Accessed May 29, 2019. https://www.huntonprivacyblog.com/2017/02/09/dpa-argentina-issues-draft-data-protection-bill/.

"Facebook Newsroom," 2019. Accessed October 27, 2019. https://newsroom.fb.com/company-info/.

Federal Law No. 242-FZ on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-

Telecommunication Networks, 2014. Accessed February 21, 2018. https://pd.rkn.gov.ru/authority/p146/p191/.

G20 Osaka Leaders' Declaration, 2019. Accessed January 1, 2020. https://www.consilium.europa.eu/en/press/press-releases/2019/06/29/g20-osaka-leaders-declaration/.

"GDPR - Our Expert Answers Your Questions – What Are OVH's Commitments in Terms of Data Location?" *OVH*. Accessed February 7, 2019. https://www.ovh.co.uk/personal-data-protection/faq.xml.

General Agreement on Trade in Services, Marrakesh Agreement Establishing the World Trade Organization. Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167, 1994.

Guidelines for Nigerian Content Development in Information and Communications Technology (ICT), 2013. Accessed January 18, 2018. https://nlipw.com/wp-content/uploads/Guidelines-for-Nigerian-Content-Development-in-Information-and-Communications-Technology-ICT.pdf.

"IBM Becomes First Company Certified Under APEC Cross Border Privacy Rules." *IBM*. Last modified August 12, 2013. Accessed August 19, 2019. www-03.ibm.com/press/us/en/pressrelease/41760.wss.

Letter from Apple, Facebook, Google, Microsoft and Oath to Senators of the US Congress Orrin Hatch, Christopher Coons, Lindsey Graham, and Sheldon Whitehouse of 6 February 2018, 2018. Accessed May 6, 2019. https://blogs.microsoft.com/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf.

Letter from Göran Marby, ICANN's President and Chief Executive Office, to William Debeuckelaere, President of the Belgium Data Protection Authority, 2019. Accessed March 11, 2019. https://www.icann.org/en/system/files/correspondence/marby-to-debeuckelaere-25jan19-en.pdf.

Letter from Marby Göran, ICANN's President and Chief Executive Officer, to Willem Debeuckelaere, President of the Belgian Data Protection Authority and to Helen Dixon, Data Protection Commissioner for Ireland, 2018. Accessed March 11, 2019. https://www.icann.org/en/system/files/correspondence/marby-to-debeuckelaere-dixon-06dec18-en.pdf.

Letter from MEPs Jan Albrecht, Bernd Lange, Viviane Reding and Marietje Schaake to President Juncker, 2016. Accessed June 28, 2020. https://marietjeschaake.eu/en/data-flows-letter-to-president-juncker.

Letter from Willem Debeuckelaere, President of the Belgian Data Protection Authority, to Göran Marby, ICANN's President and Chief Executive Officer, 2019. Accessed March 11, 2019. https://www.icann.org/en/system/files/correspondence/debeuckelaere-to-marby-15jan19-en.pdf.

"Meeting the Challenge of Data Localization Laws." *Servers.Global*, November 30, 2016. Accessed December 31, 2017. https://www.servers.global/meeting-the-challenge-of-data-localization-laws/.

Memorandum of Understanding between the Privacy Commissioner of Canada and College Bescherming Persoonsgegevens on Mutual Assistance in the Enforcement of Laws Protecting Personal Information in Private Sector, 2011. Accessed April 15, 2019. https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-memorandums-of-understanding/mou-netherland/.

"Merck Successfully Concludes First APEC-Based BCR Approval." *TrustArc Blog*. Last modified March 22, 2016. Accessed August 20, 2019. https://www.trustarc.com/blog/2016/03/22/merck-successfully-concludes-first-apec-based-bcr-approval/.

"Merkel and Hollande Mull Secure European Communication Web." *Deutsche Welle*. Last modified February 16, 2014. Accessed December 31, 2017. http://www.dw.com/en/merkel-and-hollande-mull-secure-european-communication-web/a-17435895.

"Nigeria Issues New Data Protection Regulation." *Privacy & Information Security Law Blog*. Last modified April 5, 2019. Accessed June 5, 2019. https://www.huntonprivacyblog.com/2019/04/05/nigeria-issues-new-data-protection-regulation/.

Oxford English Dictionary. 3rd ed., 2011.

"President Donald J. Trump Announces Intent to Nominate Individual to Key Administration Posts." *The White House*. Accessed April 27, 2019. https://www.whitehouse.gov/presidential-actions/president-donald-j-trump-announces-intent-nominate-individual-key-administration-posts/.

"Search Engine Market Share." Accessed October 27, 2019. https://goo.gl/vb1Gof.

"Thailand's National Legislative Assembly Passes Data Protection Law." *Privacy & Information Security Law Blog*. Last modified March 15, 2019. Accessed June 5, 2019. https://www.huntonprivacyblog.com/2019/03/15/thailands-national-legislative-assembly-passes-data-protection-law/.

"United Nations Declares Internet Access a Human Right; Cuba, Venezuela Oppose Move." *Fox News*. Last modified July 6, 2016. Accessed January 26, 2018. http://www.foxnews.com/politics/2016/07/06/un-resolution-declares-internet-access-human-right-cuba-venezuela-oppose-it.html.

"U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Federal Privacy Law." *U.S. Chamber of Commerce*. Last modified February 13, 2019. Accessed May 25, 2019. https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law.

"What Is the Brazil General Data Protection Law (LGPD)?" *OneTrust*, July 20, 2018. Accessed May 24, 2019. https://www.onetrust.com/what-is-the-brazil-general-data-protection-law-lgpd/.

"Where Your Data Is Located." *Microsoft Trust Center*. Accessed January 20, 2018. https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located.

"With the Future of the US-EU Data Privacy Shield in Doubt, Companies Are Considering Other Options." *CMS*. Last modified October 29, 2018. Accessed January 17, 2019. https://www.cms-lawnow.com/ealerts/2018/10/with-the-future-of-the-us-eu-data-privacy-shield-in-doubt-companies-are-considering-other-options.

Table of cases

Court of Justice of the European Union

Judgment of 25 November 1971, *Béguelin Import v G.L. Import Export*, C-22/71, ECLI:EU:C:1971:113.

Judgment of 4 July 1985, *Berkholz v Finanzamt Hamburg-Mitte-Altstadt*, C-168/84, ECLI:EU:C:1985:299.

Judgement of 27 September 1988, *Ahlström Osakeyhtiö and Others v Commission*, Joined Cases 89/85, 104/85, 114/85, 116/85, 117/85 and 125/85 to 129/85, EU:C:1988:447.

Judgement of 9 July 1992, *Commission v Belgium*, C-2/90, ECLI:EU:C:1992:310.

Judgment of 7 May 1998, *Lease Plan Luxembourg v Belgische Staat*, C-390/96, ECLI:EU:C:1998:206.

Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

Judgment of 7 December 2010, *Pammer and Hotel Alpenhof*, Joined Cases C‑585/08 and C‑144/09, ECLI:EU:C:2010:740.

Judgment of 12 July 2011, *L'Oréal and Others*, C-324/09, ECLI:EU:C:2011:474.

Judgment of 21 December 2011, *Air Transport Association of America and Others*, C-366/10, ECLI:EU:C:2011:864.

Opinion of Advocate General Jääskinen delivered on 25 June 2013, *Google Spain and Google*, C-131/12, ECLI:EU:C:2013:424.

Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317.

Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639.

Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.

Action brought on 16 September 2016, *Digital Rights Ireland v Commission*, Case T-670/16.

Action brought on 25 October 2016, *La Quadrature du Net and Others v Commission*, Case T-738/16.

Judgment of 6 September 2017, *Intel Corp. v European Commission*, C-413/14 P, ECLI:EU:C:2017:632.

Order of the General Court of 22 November 2017, *Digital Rights Ireland v Commission*, Case T-670/16, ECLI:EU:T:2017:838.

Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, Case C-311/18.

Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, *Facebook Ireland and Schrems*, Case C-311/18.

France

L'Union Des Etudiants Juifs De France Et La Ligue Contre Le Racisme Et L'Antisemitisme v. Yahoo! Inc. et Yahoo! France, T.G.I. Paris, May 22, 2000, No. RG: 00/05308.

United States

Microsoft v. United States, 829 F.3d 197 (2d Cir. 2016).

International case-law

Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 6, 35 (Apr. 9).