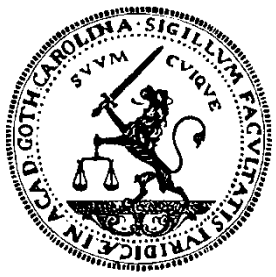

FACULTY OF LAW
Lund University

Au Nguyen Thi Hai

The Future of International Data Transfers and the Safeguards for International Corporations after Schrems II

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Eduardo Gill-Pedro

Term: Spring 2022

Table of Content

Abstract

The EU-US Privacy Shield Decision on data transfers between the EU and the US was found invalid by the CJEU Schrems II ruling on 16 July 2020. After Schrems II, discussions among scholars and practitioners on legal challenges of international data transfers resulting from the case has gained much tension during the past years. Given the significant amount of data that flows between organizations around the world - particularly between the EU and the US, the Schrems II judgment and current EU's data transfer mechaninsms have upended many multinational companies' data protection policies and practices. This leads to considerable uncertainty in the regulatory landscape of cross-border data transfers post-Schrems II. This thesis, therefore, aims to examine how the EU's current data protection regulatory frameworks address data protection and privacy issues raised following the Schrems II ruling on cross-border transfers of EU personal data to a third country outside the EU/EEA, from the perspective of multinational corporations.

This thesis finds that after Schrems II, international data transfer rules have changed. Companies cannot continue to base on the adequacy decision Privacy Shield to conduct trans-Atlantic data transfers. The use of the new SCCs to transfer data to a third country outside the EU/EEA was upheld by the CJEU, but it must ensure a level of protection that is 'essentially equivalent' to that in the EU. The new legal requirements that contained Transfer Impact Assessment - the TIA for each data transfer outside the EU/EEA, requires both exporters and importers must now be more active in ensuring data transfer compliance as it places more obligations on them. There are not only higher standards of protection for cross-border data transfers but also enhanced role of the DPAs implementation enforcement, which leads to greater uncertainty for multinationals.

Chapter V of the GDPR provides some potential choices as alternatives for multinational companies other than the Privacy Shield and the new SCCs, such as, Binding Corporate Rules - BCRs, approved Codes of Conduct/Certification, consent and the derogations as set out in Article 49 of the GDPR. This thesis also includes a discussion of data localization as a solution to the issue at hand. It concludes that while waiting for EU-level legislation and policy development, what multinational companies can do to remain compliant with the EU law when transferring personal data outside the EU/EEA is that they can keep using the new SCCs and the BRCs (or otherwise the alternative mechanisms that are practically available). While doing so, they need to perform their own Data Privacy Impact Assessment - DPIA and the TIA following the EDPB Recommendations and the GDPR.

Keywords: EU, Internal Market, GDPR, EU Law, Privacy, Data Protection, Schrems, Cross-border Data Transfers, Privacy Shield, New SCCs, Data Localization.

Preface

There would be no Lund and Sweden and this master's thesis without my family and Tran Ba Thong, my pillars of support. Thank you, my family, my loved ones, thank you for always being there for me. I am so grateful for the unwavering support that you have given me in every decision I have. Without you, my path would be very different. Thank you, Tran Ba Thong, my high school sweetheart. You have always encouraged me to do my best and with you, there is nothing impossible. I don't know how much to say, but I am so grateful we have each other.

I could not have made it through the past two years away from home, Covid-19 and social distancing, a new continent and new people, without my dearest friends Maricar Joy Tuazon and Hano Sabir, Vo Hoang Yen Linh and Tran Huy Cuong. Thank you for being there for me in this challenging period. It has been a fantastic journey with you! We've been through two such long winters, which seemed long but turned out to be short... Thank you all! Special thanks to Xuhoa, my dear ex-colleague, you are my lifesaver, and you know it!

This master's thesis would not be complete as it is today without the dedicated guidance, feedback, and opinions from my supervisor, Eduardo Gill-Pedro. Thank you for your input and the online and offline meetings you shared so enthusiastically of your valuable time. I would also want to give a special "thank you" to my professors Xavier Groussot and Julian Nowag. Thank you for your kindness and support. It meant a lot to me.

Finally, I would like to express my deep gratitude to the entire Lund University Law Faculty and all my classmates - the class of 2020-2022 LLM in EU Business Law, despite the difficulties and unusual circumstances brought about by the Covid-19 pandemic, the experiences of studying with you at the Faculty of Law and at Lund University are all that I will treasure for many years to come. Thank you!

Lund, 21 May 2022
Au Nguyen

Abbreviations

BCRs	Binding Corporate Rules
CFR	Charter of Fundamental Rights of the European Union
CIA	The US Central Intelligence Agency
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
DPIA	Data Privacy Impact Assessment
EC	European Commission
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
EEA	European Economic Area
EDPB	European Data Protection Board
EU	European Union
FBI	The US Federal Bureau of Investigation
GDPR	General Data Protection Regulation
NSA	The US National Security Agency
OECD	Organization for Economic Co-operation and Development
SCCs	Standard Contractual Clauses
Schrems I	Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650
Schrems II	Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd [2020] ECLI:EU:C:2020:559
TEU	Treaty of the European Union
TFEU	Treaty of the Functioning of the European Union
The US	The United States

Chapter 1. Introduction

1.1. Background

1.1.1. Data protection EU law

In the online environment, data communication is limitless. The global digital transformation makes legal landscape of privacy and data protection important at both the national and international levels to ensure the fundamental privacy rights of individuals are not compromised when multinational enterprises exploiting personal data for data-driven business activities. In principle, when it comes to data protection rules of the European Union (hereinafter referred to as the EU) on cross-border data transfers, there is a free flow of personal data within the EU. With third countries outside the EU there can be also cross-border flow of personal data *subject to conditions*, which essentially requires an appropriate level of protection in the third country concerned.[1]

For decades, the EU has held high standards of data protection law.[2] To protect EU citizens' personal data, the EU has codified the individuals' fundamental rights over their personal data and privacy in multiple EU legislations: Article 16 of the Treaty of the Functioning of the European Union (TFEU)[3] on data protection, Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (CFR)[4] on the right to privacy and the right to the protection of personal data concerning him or her, as well as in Article 6 and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[5] regarding the right of everyone to respect for their private and family life, their home and their correspondence.

The EU first adopted data protection legislation in 1995, the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on

[1] Justine Pila and Paul Torremans, *European Intellectual Property Law* (2nd edition, Oxford University Press 2019) 512.
[2] European Data Protection Supervisor (EDPS), 'Data Protection' (*EDPS*) <https://edps.europa.eu/data-protection/data-protection_en> accessed 22 March 2022.
[3] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU).
[4] Charter of Fundamental Rights of the European Union (adopted 2 October 2000, entered into force 7 December 2000) OJ C 326/291 (CFR).
[5] European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) ETS 5 (ECHR).

the free movement of such data (the Data Protection Directive)[6], which is to response to the personal data processing phenomenon.[7] As a radical step to deal with the implications of the digital age, in April 2016, the EU adopted General Data Protection Regulation (GDPR)[8] to replace the Data Protection Directive, which later became fully applicable across the EU in May 2018, targeting not only to liberalize cross-border data flows between the Member States of the EU but also to protect personal data.[9]

Cross-border data transfer has been partially managed by the EU through the issuance of adequacy decisions (Article 45 of the GDPR) as one of the data transfer tools set out in Chapter V of the GDPR. By 2022, the European Commission (the EC) has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the Law Enforcement Directive[10], and Uruguay as providing adequate protection[11]. Apart from the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of the Law Enforcement Directive)[12].

The most prominent with many fluctuations must be the adequacy decisions issued in relation to the EU-US trans-Atlantic data sharing. In particular, the

[6] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L [1995] 281/31.

[7] European Union Agency for Fundamental Rights and others, *Handbook on European Data Protection Law : 2018 Edition* (Publications Office 2018) 29 <https://data.europa.eu/doi/10.2811/343461> accessed 17 April 2022.

[8] Regulation 2016/679 of the European Parliament and of the Council of April 27, 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 [2016] 119/1 (hereinafter the GDPR).

[9] Claes Granmar, 'E-Commerce and the EU Data Protection Regulation' 1 <https://www.diva-portal.org/smash/get/diva2:1278665/FULLTEXT01.pdf> accessed 20 March 2022; European Commission (EC), 'Data Protection in the EU' (*EC*) <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en> accessed 26 March 2022.

[10] 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 4.5.2016 (Law Enforcement Directive).

[11] European Commission (EC), 'Adequacy Decisions' (*EC*) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 28 March 2022.

[12] Law Enforcement Directive (n 10).

EU–US Safe Harbor Decision 2000 (the Safe Harbor Decision)[13], which was found invalid in 2015 by the Court of Justice of the European Union (CJEU) in Schrems I[14], and the EU-US Privacy Shield Decision 2016 (the Privacy Shield Decision)[15] that the CJEU later in 2020 also invalidated in the case of Schrems II[16] by finding that the Privacy Shield Decision did not guarantee sufficient data protection in accordance with the EU law.

The CJEU judgment in Schrems II is seen as a groundbreaking ruling because in this judgment the court found that the adequate decision for the EU-US data transfer mechanism, the Privacy Shield Decision, is invalidated in its entirety[17]. The Court concluded that the United States (the US) authorities' surveillance capacities conflicted with the EU fundamental rights (under Article 45.1 of the GDPR read in the light of Articles 7, 8 and 47 of the CFR). This makes the legal landscape of cross-border data transfers uncertain as it disables the Privacy Shield Decision without specific and immediate instructions from the CJEU and EU data regulators. On the one hand, multinational corporations do not have timely and legal responses to data transmission activities for their day-to-day business. On the other hand, it also destabilizes the EU digital market and the functioning of the EU internal market, which requires prompt responses from EU lawmakers.

1.1.2. Multinational corporations and modern trans-border data flows

Data and emerging technologies play an increasingly important role in shaping internationalization as digitalization has become a key element underpinning the way multinational enterprises organize their international operations[18]. Amid the COVID-19 pandemic, new technology has effectively reshaped the organization of the global economy and how their businesses must adapt to new conditions. Working from home has become the new normal. Businesses are now functioned digitally, and the adoption of cloud

[13] Commission Decision 2000/520/EC 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 harbor privacy principles and related frequently asked questions issued by the US Department of Commerce OJ L 215, 25.8.2000, p. 7–47.
[14] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.
[15] 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 [2016] OJ L207/1 (Privacy Shield Decision).
[16] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* [2020] ECLI:EU:C:2020:559.
[17] *Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd [2020] ECLI:EU:C:2020:559* (n 2), paras 199-121.
[18] Julia Staudt Gestrin, Michael V, 'The Digital Economy, Multinational Enterprises and International Investment Policy' [2018] OECD <http://www.oecd.org/investment/the-digital-economy-mnes-and-international-investment-policy.htm> accessed 8 March 2022.

platforms is ascending. This unpredicted new reality made the implications of Schrems II ruling become more complex, especially for data-driven companies that operate on a global scale, for instance, the tech giants, also known as FANG in the US (Facebook/Meta, Amazon, Netflix, Google/Alphabet).[19]

The evolution of the Internet has made cross-border data flows increased unimaginably. According to the World Bank index, in 2020, annual *global* internet traffic was estimated to be more than 3 zettabytes, or 3,000,000,000,000 gigabytes (GB)[20]. By 2022, the yearly global total internet traffic is projected to increase by about 50 percent from 2020 levels, reaching 4.8 zettabytes, equal to 150,000 GB per second[21]. Personal data is expected to represent a significant share of the total volume of data being transferred cross-border[22]. With that said, the amount of personal data that multinationals process as an essential element in their day-to-day business operations has also grown rapidly, together with the increased need for data sharing throughout their group of companies[23].

Often, international data sharing is necessary for multinationals to manage their customer data and human resources, as well as to implement a cost-effective centralized IT function[24]. As a crucial factor of international trade, data flows not only by and between intra-group organizations but also between the company with their establishments from around the world and their external service suppliers[25]. They may, for example, have their customers' personal data stored in a third county outside the EU/EEA[26] by a cloud service provider or have their employees' personal data accessed remotely by various stakeholders at a foreign subsidiary. They may also at times outsource IT functions to third-party service providers, share data with

[19] ibid 7.
[20] The World Bank (WB), 'Data for Better Lives - Crossing Borders' (The World Bank 2021) <https://wdr2021.worldbank.org/stories/crossing-borders/> accessed 13 March 2022.
[21] ibid.
[22] ibid.
[23] EML Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (1st ed, Oxford University Press 2012) 20.
[24] Renzo Marchini, 'Data Transfers within a Multinational Group Safely Navigating EU Data Protection Rules' (*Dechert LLP*, May 2013) <https://www.lexology.com/library/detail.aspx?g=2b2f345f-a5fa-4001-98e3-f189a5441644> accessed 10 February 2022.
[25] Moerel (n 23) 21.
[26] The European Economic Area (EEA) Includes All EU Countries and Non-EU Countries Iceland, Liechtenstein and Norway. European Commission (EC), 'Rules on International Data Transfers' (*EC*) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en> accessed 10 February 2022.

international service clients, or coordinate marketing efforts with facilities in a non-EU country.[27]

The fact that multinationals have establishments in most EU Member States, the transfer of the employee and customer data of these EU establishments to non-EU ones, such as, the US and other non-EU countries, might trigger the EU data protection laws of these Member States.[28] Protecting personal data and managing international transfers of EU personal data to a third country outside of the EU has become more critical than ever for multinationals when it comes to data privacy and corporate governance.

1.1.3. The developments of the EU privacy legal landscape for international data transfer after Schrems II

As aforementioned, there are various data transfer mechanisms in place as set forth in Chapter V of the GDPR. It includes (i) *adequacy decisions* under Article 45, (ii) *supplementary safeguards* under Article 46 and (iii) *the use of one of the derogations* under Article 49[29]. The three transfer tools constitute a hierarchy according to Christopher Kuner[30]:

> *three-tiered structure for legal bases (...), with **adequacy decisions** at the top, **appropriate safeguards** in the middle, and **derogations** at the bottom. This means that if an adequacy decision has been issued then that should be relied on; if not, then appropriate safeguards should be used; and only if neither of these legal bases is available should the derogations be relied on.*[31]

The Court in Schrems II held that the Privacy Shield Decision was disabled, while the use of Standard Contractual Clauses (the SCCs) remained[32]. Following Schrems II, on 18 June 2021, the European Data Protection Board

---

[27] Klaus Julisch and Florian Widmer, 'GDPR Update: The Future of International Data Transfers' (*Deloitte*) <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-the-future-of-international-data-transfer.html> accessed 12 February 2022; Moerel (n 23) 87.

[28] Moerel (n 23) 90.

[29] Marcelo Corrales Compagnucci, Mateo Aboy and Timo Minssen, 'Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)' [2021] SSRN Electronic Journal 12 <https://www.ssrn.com/abstract=3951085> accessed 6 March 2022.

[30] As cited in P Breitbarth, 'A Risk-Based Approach to International Data Transfers' (2021) 7 European Data Protection Law Review 539, 542 <http://edpl.lexxion.eu/article/EDPL/2021/4/9> accessed 6 March 2022.

[31] Christopher Kuner, *'Article 44. General principle for transfers'* in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198826491.001.0001/isbn-9780198826491> accessed 13 March 2022.

[32] Corrales Compagnucci, Aboy and Minssen (n 29) 1.

(the EDPB) adopted the final version of the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the EDPB Recommendations)[33] that provides a six-step approach to help controllers and processors, acting as data exporters, with their complex task of assessing third countries and identifying appropriate supplementary measures where needed to ensure an essentially equivalent level of protection to the data they transfer to third countries. On 4 June 2021, the EC adopted two new sets of SCCs[34]: (i) one for use between controllers and processors in the EU/EEA (or otherwise subject to the GDPR), and (ii) one for the transfer of personal data to third countries outside the EU/EEA (and not subject to the GDPR). These new developments have raised the bar for data protection in international data transfers.

1.2. Purpose and Problem

After the *Schrems II*, discussions among scholars and practitioners on legal challenges of international data transfers resulting from the case has gained much tension during the past years. Given the significant amount of data that flows between organizations around the world - particularly between the EU and the US, the Schrems II judgment and current EU's data transfer mechaninsms have upended many multinational companies' data protection policies and practices. This leads to considerable uncertainty in the regulatory landscape of cross-border data transfers post-Schrems II. This thesis, therefore, aims to examine how the EU's current data protection regulatory frameworks address data protection and privacy issues raised following the Schrems II ruling on cross-border transfers of EU personal data to a third country outside of the EU/EEA. The research questions will be answered by this thesis are as follows:

- What are the challenges that the EU legal mechanisms on cross-border data transfer in Chapter V of the GDPR pose to the inter-functioning of the internal market following Schrems II judgment?

- What are the possible avenues that the EU law provides to enable lawful transfer of personal data and evaluate those choices from the perspective of multinational corporations on how helpful they are?

[33] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0. Adopted on 18 June 2021 (the EDPB Recommendations).

[34] European Commission (EC), 'Standard Contractual Clauses (SCC)' (*EC*) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> accessed 22 April 2022.

This thesis focuses on principles of data protection and the integrity of individuals' privacy and other regulatory rights under the EU law and how they can be applied to ensure the free and unrestricted flow of personal data, not only within the EU but also outside it. The thesis also discusses the cross-border transfers of personal data by multinational companies and the mechanisms that EU law provides so that personal data can flow freely without any hindrance. The focus will be on EU regulatory frameworks based on the principles and objectives of EU treaties; however, the approach and analysis will be taken from the perspective of multinational corporations.

1.3. Materials and Methodology

This thesis is carried out using a legal dogmatic methodology[35], a research method that entails (i) systematization of the principles, rules and concepts governing a particular legal field or institution through the construction of the legal concept; and (ii) interpretation of legislation by analyses of the relationship between these principles, rules and concepts with a view to solving unclarities and gaps in the existing law.

Having regard to the purpose, the legal dogmatic method is used to identify applicable EU law governing the subject matter, in other words, *de lege lata*, a methodology about finding what the law is, to understand the rationale behind the legal frameworks, its implications, and compatibility regarding the topic at hand[36]. For the topic of the research, the data transfer mechanisms that EU law provides to have free flows of personal data under Chapter V of the GDPR will be presented and evaluated. When evaluating these mechanisms, it will problematize them from the perspective of multinational corporations on how helpful they are, as well as on how suitable they will be to be used by multinational companies to conduct the cross-border data transfer.

This thesis then makes use of a methodology that helps clarify what the law should be like and how the law is enforced, *de lege ferenda*, together with criticizing the system – current legal rules, as well as proposing a 'new way' to overcome the current situation – solutionism[37], where possible, to facilitate

---

[35] Jan M Smits, 'What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' [2015] SSRN Electronic Journal 5 <http://www.ssrn.com/abstract=2644088> accessed 14 March 2022.

[36] Mark Van Hoecke, *Methodologies of Legal Research: What Kind of Method for What Kind of Discipline?* (Hart Publishing 2011) 8 <http://www.bloomsburycollections.com/book/methodologies-of-legal-research-what-kind-of-method-for-what-kind-of-discipline> accessed 14 March 2022.

[37] Rob van Gestel and Hans-Wolfgang Micklitz, 'Why Methods Matter in European Legal Scholarship: Methods in European Legal Scholarship' (2014) 20 European Law Journal 292 <https://onlinelibrary.wiley.com/doi/10.1111/eulj.12049> accessed 14 March 2022.

the operations of multinationals in the digital era. This can be implemented by systemizing and interpreting authorized legal sources of the EU law, including the EU and Member States' primary and secondary laws.

Since the EU is based on the rule of law, the EU Treaties are the starting point for EU law.[38] The EU Treaties, which have been ratified by all EU Member States[39], consist of the Treaty of the European Union (TEU) and TFEU; the CFR of the EU and the ECHR, they form the EU primary law and considered to be a binding source.[40]

The body of law that comes from the principles and objectives of the Treaties is known as EU secondary law; and includes regulations, directives, decisions, recommendations, and opinions.[41] These sources of law are binding, and they shall not be disregarded.[42]

In addition to the EU primary and secondary sources of law, this thesis also makes use of online journals and articles of legal scholars, as well as reports produced for the reference of the EU and relevant EU authorities to get a deeper understanding of the topic. Most notably, contemporary opinions and updates on the two occurring events[43] introduced in this thesis will also be included to contribute to the point of view of the topic.

1.4. Definition and Disposition

Regardless of the ongoing information explosion and the growth in the complexity and volume of the data being transferred cross-border in a global scale, it is difficult to define what constitutes a 'data transfer' and 'cross-border data transfer'. There are different terms variously used in regulatory instruments to describe it[44]. For example, as Kristopher Kuner lists out in his

---

[38] European Commission (EC), 'Types of EU Law' (*EC*) <https://ec.europa.eu/info/law/law-making-process/types-eu-law_en#:~:text=Treaties%20are%20the%20starting%20point,%2C%20decisions%2C%20recommendations%20and%20opinions.> accessed 22 March 2022.

[39] After the withdrawal of the United Kingdom from the EU at 23:00 GMT on 31 January 2020, the EU has total 27 member states.

[40] Paul Craig and G De Búrca, *EU Law: Text, Cases, and Materials* (Sixth edition, Oxford University Press 2015) 266.

[41] European Commission (EC), 'Types of EU Law' (n 38).

[42] Craig and De Búrca (n 40) 266.

[43] Including: (i) Decision of Austria's DPA ruling that the continuous use of Google Analytics violates the GDPR, and (ii) French CNIL's Decision on the EU-US data transfers through the use of analytics cookie to be unlawful.

[44] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 11 <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199674619.001.0001/acprof-9780199674619> accessed 10 April 2022.

book[45], the Chapter V of the GDPR refers to 'data transfer to the third country' without defining what is 'data transfer', the Organization for Economic Co-operation and Development (OECD) Guidelines[46] refers to 'transborder data flows' as 'movements of personal data across national borders', while the Council of Europe Convention 108[47] uses the terms 'transborder flows of personal data' to refer to 'the transfer of [personal] data to a recipient who is subject to the jurisdiction of another Party to the Convention'[48].

In his book, Kristopher Kuner uses the terms 'transborder data flows' and defines it as 'the term to generically to all cases of data crossing national border'[49]. While Kristin Archick and Rachel F Fefer refer to 'cross-border data flows' as 'the movement or transfer of information between computer servers across national borders, which is of importance in conducting international trade and commerce.[50] To avoid any confusion, in this thesis, the terms *'international data transfers'*, *'cross-border data transfers'*, '*transborder data flows'* or *'cross-border data flows'* are used interchangeably to describe the transfer of personal data of individuals across borders in the networked environment.

This thesis consists of five chapters:

(i) *The first chapter* gives an introduction about the background and presents the topic.
(ii) *The second chapter* will deepen into the internal market and EU regulations on cross-border data transfers.
(iii) *The third chapter* looks at current cross-border data transfer mechanisms under the EU data protection law - Chapter V of the GDPR, as well as the six-step approach recommendations by the EDPB. It will also look further into the type of accountability

[45] ibid.
[46] OECD, 'Personal Data Protection at the OECD' (*Organisation for Economic Co-operation and Development (OECD)*) <https://www.oecd.org/general/data-protection.htm> accessed 12 April 2022.
[47] Modernized Convention for the Protection of Individuals with regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session of the Committee of Ministers (Elsinore, 18 May 2018) (Convention 108). Available at <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf> accessed 15 April 2022.
[48] Article 14.1 of the Convention 108.
[49] Kuner (n 44) 11.
[50] Kristin Archick and Rachel F Fefer, 'U.S.-EU Privacy Shield and Transatlantic Data Flows' (Congressional Research Service (CRS) 2021) R46917 5 <https://crsreports.congress.gov/product/pdf/R/R46917#:~:text=Since%20the%20media%20leaks%20of,Privacy%20Shield%20Framework%2C%20in%202020.> accessed 22 March 2022.

requirements of data exporters and importers as well as the various organizational and technical measures, mainly provided by the new SCCs, to understand its state of implementation on cross-border data transfers, which may help organizations tailor the right response.

(iv) In *the fourth chapter*, Schrems I and II judgments and the aftermath will be presented, including major implications of Schrems II beyond the EU-US data transfers and the impact of Schrems II in reaching agreement on possible adequacy decisions - Privacy Shield 2.0 for the US.

(v) *The final chapter* includes discussions about the topic from different perspectives. From the organizational level, how does multinational companies tailor the right response to its difficult position? From the EU level, whether data localization a solution for the EU? It is also an effort to answer the research questions, which includes the analysis of the various areas of the issues being examined and concluding the thesis findings.

Chapter 2. Internal market and the EU regulations on cross-border data transfers

2.1. Internal market and EU data protection law

The common market created by the Treaty of Rome in 1958 was intended to eliminate trade barriers between Member States with the aim of increasing economic prosperity and contributing to 'an ever-closer union among the peoples of Europe'.[51] One of the goals set by the EU in Article 3.3 TEU is that: 'The Union shall establish an internal market'. The internal market has been created and defined in Article 26.2 TFEU as an 'area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of this Treaty'. For a high level of harmony in the regulatory environment and therefore frictionless trade across the member states, the EU has integrated the internal market by adopting common standards and harmonizing the laws of the Member States.[52]

With the growing role of digital technologies and the emergence of data processing industry in the EU, the European Parliament called for data protection legislation as early as in the mid-1970s. By 1990, the EC was concerned that various national data protection laws would hinder the functioning of the internal market, the EC proposed the Data Protection Directive to regulate the processing of personal data in the EU.[53] In 1995, the Data Protection Directive was adopted to harmonize the EU law on data protection and improve the functioning of the internal market, as well as to address the gaps in Member State legislation on the protection of fundamental rights[54]. The Data Protection Directive sets its objective to 'protect the

[51] 'The Internal Market: General Principles' (*Fact Sheets on the European Union - 2022*) 1 <https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.1.1.pdf> accessed 4 May 2022.
[52] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (1st edn, Oxford University Press 2020) 67 <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190088583.001.0001/oso-9780190088583> accessed 17 April 2022.
[53] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law 65, 70 <https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501> accessed 26 March 2022.
[54] Sofija Voronova and Anna Nichols, 'Understanding EU Data Protection Policy' (*European Parliamentary Research Service (EPRS)*, May 2020) 3

fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'[55], and another objective that neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection of personal data and privacy[56].

The right to privacy and the right to protection of personal data are both enshrined in the CFR and the EU Treaties. The entry into force of the Lisbon Treaty in 2009 gave the Charter the same legal value as the Treaties (Article 6.1 TEU), which provides a stronger basis for a more effective and comprehensive data protection regime in the EU.[57] After the entry into force of the Lisbon Treaty, Article 16.1 of the TFEU establishes the right to protection of personal data: 'everyone has the right to the protection of personal data concerning him or her'. Articles 7 and 8 of the CFR provide for a right to privacy and a right to protection of personal data respectively. Article 8 of the ECHR also provides a right to respect for private and family life. It is to be noted that corresponding rights under the CFR and the ECHR have the same meaning and scope as provided in the Article 52.3 of the ECHR.

The GDPR was adopted in 2016 and fully applied in 2018, repealing the Data Protection Directive and becoming the main EU legal instrument for personal data protection. The GDPR sits in the structure of objectives of the EU. It is not only part of the internal market policy but also the common commercial policy. The internal market was established for the common goals of the Member States, but it is not a closed market. With the aim of enhancing trade between the EU and their bargaining power with the rest of the world, EU Member States delegate authority to the EC to negotiate their external trade relations, the so-called Common Trade Policy of the EU. Article 3.1 of the TFEU provides that the EU has exclusive competence in the common commercial policy. In this regard, Recital 101 of the GDPR acknowledges the importance of personal data flows to and from countries outside the EU and international organizations for the expansion of international trade and international cooperation of the EU.

2.2. Data Protection Directive and the GDPR

<https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf> accessed 5 May 2022.

[55] Article 1.1, Data Protection Directive.

[56] Article 1.2, Data Protection Directive.

[57] Voronova and Nichols (n 53) 1.

In the context of the Council of Europe[58], all EU Member States have all signed up to Convention 108, a convention in 1981 for the protection of individuals with regard to automatic processing of personal data[59]. In principle, Convention 108 applies to all data processing carried out by both the private and public sectors, including data processing by the judiciary and law enforcement authorities.[60] Convention 108 later underwent the modernization process carried out in 2011, in parallel with the reform of EU data protection rules which was launched in 2012 when the EC proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy[61].

The EU data protection reform resulted in the adoption of new EU data protection rules, the *GDPR* which replaced the Data Protection Directive, and the *Law Enforcement Directive*[62] for the law enforcement and police area.[63] They entered into force in May 2016 and took full legal effect across the EU and subsequently the EEA, together comprising 31 countries, in May 2018.[64] The reform is a radical step towards modernizing and harmonizing data protection across the EU.[65] It is an essential element of the ambitious Single Digital Market Strategy, which aims to help the EU maintain its position as a world leader in the digital economy field, as well as help EU companies grow globally.[66]

Recital 1 of the GDPR highlights that privacy and data protection are fundamental rights of the EU. It refers to Article 8.1 of the CFR as the core of the right to data protection as a fundamental right, along with Article 16.1 of the TFEU, according to which 'everyone has the right to the protection of personal data concerning him or her'. Article 16.2 of the TFEU mandates the EU to act in privacy and data protection within the EU. The first is that it empowers the European Parliament and the EC to issue EU data protection

[58] The Council of Europe is the continent's leading human rights organization. It comprises 47 member states, 28 of which are members of the European Union. See further Convention 108, available at <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf> accessed 15 April 2022.
[59] Pila and Torremans (n 1) 498.
[60] ibid; European Union Agency for Fundamental Rights and others (n 7) 24.
[61] European Union Agency for Fundamental Rights and others (n 7) 26.
[62] Law Enforcement Directive (n 10).
[63] European Commission (EC), 'Data Protection in the EU' (n 9).
[64] ibid.
[65] Burri and Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 Journal of Information Policy 479, 480 <http://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0479> accessed 19 April 2022.
[66] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, a Digital Single Market Strategy for Europe, COM/2015/0192 final.

rules in accordance with the ordinary legislative procedure[67]. Additionally, it obliges the EU to give the independent data protection authorities the task of ensuring control of the rules on data protection[68]. With that said, Article 16 of the TFEU confers wide powers on the EU to regulate EU data protection rules yet leaves room for national legislation. The Member States remain important actors in this field of practice.[69]

The new data protection regulations provided by the GDPR became vital as it substantially enhances the rights of data subjects with requirements for greater transparency, the right to access the information and the right to be forgotten, and other data subjects' rights[70]. On top of it, the GDPR deals with the transfer of personal data to third countries or international organizations in a separate chapter - Chapter V, which highlights a set of conditions requiring the third country to ensure an adequate level of protection when performing such transfers.

Since then, the GDPR has become an effective regulatory tool both at the EU level and the global one for data protection and the transfer of personal data across borders. On the one hand, as a binding form of EU law that is capable of direct effect[71], the GDPR provides a single set of data protection rules across the EU. This creates consistent data protection rules throughout the EU and reinforces legal certainty of the EU legislation environment from which economic operators and individuals as "data subjects" may benefit[72]. On the other hand, the wide scope of application that the GDPR catches under its net makes it applicable to all businesses and organizations operating both domestically and outside the EU whose activities touch the EU in the sense it sets forth in Article 3.[73]

Not only has the EU succeeded in achieving harmonization among its Member States in different areas, but also the EU law has extended its sphere of influence at the international level to other countries and territories. In the field of data protection and privacy, the world has witnessed the influence of EU legal regulations on the global data protection regulatory frameworks by having the EU shape the global norms for data protection[74]. The phenomenon

[67] Article 16.2 TFEU, first paragraph, first sentence.
[68] Article 16.2 TFEU, first paragraph, second sentence.
[69] Hielke Hijmans, 'The Mandate of the EU Under Article 16 TFEU and the Perspectives of Legitimacy and Effectiveness' in Hielke Hijmans, *The European Union as Guardian of Internet Privacy*, vol 31 (Springer International Publishing 2016) 128 <http://link.springer.com/10.1007/978-3-319-34090-6_4> accessed 19 April 2022.
[70] Pila and Torremans (n 1) 506–508.
[71] Craig and De Búrca (n 40) 198.
[72] European Union Agency for Fundamental Rights and others (n 7) 30.
[73] Pila and Torremans (n 1) 502–503.
[74] Bradford (n 51) 17.

of the global dissemination of EU data protection standards, which, according to Anu Bradford in her famous work - the so-called Brussels Effect[75] - has been concurred and supported by the existing literature.[76]

2.3. Summary

This chapter provides an overview of the internal market and EU regulations on cross-border data transfers. It is opened with a short introduction to the EU and its objectives, the introduction of the internal market and EU data protection legislation. This section summarizes the EU's data protection law and the EU's early response to the emerging digital technology and emergence of the data processing industry in the EU, including the enactment of the Data Protection Directive as the EU's first regulation on data protection. The objective of the Data Protection Directive is not only to protect the right to privacy of individuals with respect to the processing of personal data, but also to ensure that matters connected with the protection of personal data and privacy will not restrict nor prohibit cross-border data flows. The GDPR later replaced the Data Protection Directive and became the main tool to govern data and privacy protection and the transferring of personal data not only within the EU but also from the EU to other countries outside the EU.

This chapter aims to present EU law as a legal order of international law with a focus on privacy and data protection. It is the claim of the concept of the autonomy of the EU legal order that has been employed by the EU Court of Justice, a new legal order that is autonomous from both the Member States' law and international law. Starting with the establishment of the internal market and the EU Treaties, this chapter then introduces the EU's objective of achieving harmonization among the Member States in various areas, including legislation on data protection to ensure the integrity of the privacy of individuals. With EU influence on global standards for data protection, EU data protection legislation and the phenomenon of the Brussels Effect are also presented.

[75] ibid 7.
[76] Marco Luisi, 'GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion' (9 April 2022) <https://www.e-ir.info/2022/04/09/gdpr-as-a-global-standards-brussels-instrument-of-policy-diffusion/> accessed 14 April 2022.

Chapter 3. EU data transfer tools

3.1. Personal data transfers within the EU and to third countries outside the EU

Throughout the EU, there is free movement of personal data without any restrictions between EU Member States. The area of free data flow has been expanded by the Agreement on the European Economic Area (EEA)[77], bringing Iceland, Liechtenstein, and Norway to participate in the internal market (hereafter collectively called the EU).[78] All members of the EEA are also parties to Convention 108. However, not all contractual parties to Convention 108 are Member States of the EU.[79]

Personal data is transferred from the EU to third countries outside the EU or international organizations only if certain conditions are met for the protection of personal data under Chapter V of the GDPR. It requires special safeguards to ensure that the protection travels with the data.[80] For this, it requires either the third country to ensure a sufficient level of protection, or the data controller or processor to provide appropriate safeguards, including enforceable data subject rights and legal remedies, such as standard contractual clauses or binding corporate rules.

Given the large volume and complexity of cross-border transfers of personal data, the GDPR provides data protection that goes with personal data and places high demands on the data protection standards during the process of data being transferred to a third country that is not a member of the EU (referred to as the 'third country' according to the GDPR). Regardless of where the data goes, EU data protection rules apply[81], thanks to the GDPR's very broad territorial scope of application[82].

---

[77] Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation, OJ 1994 L 1.
[78] European Union Agency for Fundamental Rights and others (n 7) 252.
[79] ibid 251.
[80] European Commission (EC), 'Rules on International Data Transfers' (n 26).
[81] European Commission (EC), 'What Rules Apply If My Organisation Transfers Data Outside the EU?' (*EC*) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en> accessed 20 April 2022.
[82] Pila and Torremans (n 1) 502.

As stated in its title, the GDPR aims at the protection of *natural persons* regarding (i) the processing of their personal data and (ii) on the free movement of such data. The GDPR is not concerned with any kind of data, but rather 'personal data', which is 'any information relating to an identifiable or identifiable natural person' (the so-called 'data subject') under Article 4.1 GDPR. The GDPR involves, on the one hand, the data subjects whose data is being processed; and controllers or processors, the two subjects that perform the processing of personal data, either for themselves (the controllers) or on behalf of the controllers (the processors), on the other hand.[83]

Simply put, the territorial scope under Article 3 of the GDPR provides that the GDPR applies when (i) data controller or data processor is established within the EU, 'regardless of whether the processing takes place in the Union or not'[84], and (ii) even when they are not established in the EU[85]. This gives the GDPR the extraterritorial scope, and it obliges many foreign companies whose activities touch the EU to be compliant.[86] While Chapter III and Chapter IV of the GDPR deal with the rights of data subjects and data controller and processor, Chapter V provides regulatory mechanisms to facilitate the transfers of personal data to third countries or international organizations.

3.2. The EU data transfer tools to third countries outside the EU

3.2.1. Chapter V of the GDPR

In principle, the EU data protection law on cross-border data transfers requires that personal data of the EU's citizens can only be transferred to the jurisdiction of a third country outside the EU if the data subject receives data protection at the level essentially equivalent to those offered under EU law[87]. The mechanisms for cross-border data transfers from the EU to third countries outside the EU provided by Chapter V GDPR include (i) adequacy decisions under Article 45 of the GDPR, (ii) appropriate safeguards under Article 46 of

[83] Article 4.7 and 4.8 GDPR.
[84] Article 3.1 GDPR.
[85] Article 3.2 GDPR.
[86] Pila and Torremans (n 1) 503.
[87] Maria Helen Murphy, 'ASSESSING THE IMPLICATIONS OF *SCHREMS II* FOR EU–US DATA FLOW' (2022) 71 International and Comparative Law Quarterly 245 <https://www.cambridge.org/core/product/identifier/S0020589321000348/type/journal_article> accessed 28 March 2022; Joseph Liss and others, 'Demystifying *Schrems II* for the Cross-Border Transfer of Clinical Research Data' (2021) 8 Journal of Law and the Biosciences lsab032 <https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsab032/6407729> accessed 29 March 2022.

the GDPR and (iii) the use of one of the derogations under Article 49 of the GDPR.

(a) Adequacy decisions under Article 45 GDPR

Article 45 of the GDPR provides the EC with a process to determine and grant 'adequacy decision' in case a particular third country ensures the adequate level of protection guaranteed within the EU to communicate personal data directly at a specific recipient[88]. Such decision allows free flow of personal data from the EU/EEA to that third country without any further necessary safeguards or being subjected to additional conditions. In other words, the transfers to an 'adequate' third country will be comparable to a transmission of data within the EU, which is so-called 'assimilated to intra-EU transmissions of data' and brings significant economic benefits.[89]

(b) Appropriate safeguards under Article 46 GDPR

In the absence of an adequacy decision, Article 46 of the GDPR stipulates that transmission of personal data to a third country or an international organization can take place only if (i) the controller or processor has provided appropriate safeguards, and (ii) on condition that enforceable rights and effective legal remedies for data subjects are available. Such appropriate safeguards can be established by:

(i) a legally binding and enforceable instrument between public authorities or bodies[90];
(ii) binding corporate rules[91];
(iii) standard data protection clauses adopted by the EC or supervisory authority[92];
(iv) codes of conduct or certification mechanism[93] together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data;
(v) customized contractual clauses between the controller or processor in the EU and the data recipient in a third country that

[88] Article 45 GDPR.
[89] European Commission (EC), 'Adequacy Decisions' (n 11); European Commission (EC), 'What Rules Apply If My Organisation Transfers Data Outside the EU?' (n 80).
[90] Article 46.2(a) GDPR.
[91] Article 46.2(b) GDPR.
[92] Article 46.2(c)(d) GDPR.
[93] Article 46.2(e)(f) GDPR.

is subject to authorization from the competent supervisory authority.[94]

(c) The use of one of the derogations listed in Article 49 GDPR

Finally, in the absence of either an adequacy decision or appropriate safeguards for a transfer of personal data from the EU to a third country, such transfer can be made based on one of the derogations for specific situations listed in Article 49 of the GDPR. For example, where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer[95], or where the transfer is necessary to perform a contract between the data subject and the controller or to implement pre-contractual measures as per data subject's request[96].

3.2.2. The six-step approach recommendations by the EDPB

After the first version was adopted in November 2020 following the CJEU Schrems II ruling, the EDPB adopted a final version of the EDPB Recommendations on supplementary measures following public consultation[97]. These recommendations provide exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place in order for them to identify and implement appropriate supplementary measures where needed to ensure an essentially equivalent level of protection to the data they transfer to third countries[98].

Step 1: Know your data transfers. This is an essential first step to fulfil data exporters' obligations under the principle of accountability. To do so, data exporters must be fully aware of their transfers by recording and mapping all transfers. The Recommendations state that data mapping must include

[94] Article 46.3(a) GDPR.
[95] Article 49.1(a) GDPR.
[96] Article 49.1(b) GDPR.
[97] EDPB, 'EDPB Adopts Final Version of Recommendations on Supplementary Measures, Letter to EU Institutions on the Privacy and Data Protection Aspects of a Possible Digital Euro, and Designates Three EDPB Members to the ETIAS Fundamental Rights Guidance Board' (*EDPB_Press Release*, 21 June 2021) <https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en> accessed 20 April 2022.
[98] ibid; EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0. Adopted on 18 June 2021 (the EDPB Recommendations). (n 33) 3.

onward transfers[99] and sub-processing chains; and such recording and mapping all transfers can be a complex exercise. It is also highlighted that (i) remote access by an entity from a third country to data located in the EEA (for example in support situations), and/or (i) storage in a cloud situated outside the EEA offered by a service provider, is also considered a transfer.[100]

Step 2: Identify the transfer tools you are relying on. Article 46 GDPR provides a list of transfer tools containing "appropriate safeguards" that exporters may use to transfer personal data to third countries in the absence of adequacy decisions (as discussed in the previous section). When choosing Article 46 GDPR transfer tools, data exporters must ensure that the transferred personal data will benefit from an essentially equivalent level of protection. The situation in the third country of the data recipient may still require that the transfer tools need additional 'supplementary measures' to ensure an essentially equivalent level of protection.[101] Only in some cases will data exporters be able to rely on one of the derogations provided for in Article 49 GDPR, if they meet the conditions. Those cases are restricted to specific situations and cannot become "the rule" in practice.[102]

Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is 'effective' in light of all circumstances of the transfer. If exporters rely on one of the transfer tools under Article 46 GDPR, they need to perform an assessment to verify if such Article 46 GDPR transfer tool is 'effective' in light of national law of the third country and practice of the importer.[103] 'Effective' means that the level of protection is essentially equivalent to that afforded in the EU[104]. Such assessment should be focused on the concerned third country legislation and the Article 46 GDPR transfer tool you are relying on, as well as the practices of the third country's public authorities. This is the so-called Transfer Impact Assessment (TIA), which will be discussed in more detail in Chapter 4.

Step 4: Identify and adopt supplementary measures. If the TIA reveals that the concerned Article 46 transfer tool is not 'effective', exporters need to consider if 'supplementary measures' exist. The EDPB Recommendations contain (in Annex 2) a non-exhaustive list of examples of supplementary measures with some of the conditions they would require to be 'effective'. As

[99] For instance, where the data processors outside the EEA transfer personal data entrusted by the data exporter to their sub-processor in another third country or in the same third country.
[100] EDPB Recommendations (n 33) 3.
[101] C-311/18 (Schrems II), paras 130 and 133.
[102] EDPB Recommendations (n 33) 3.
[103] ibid 3–4.
[104] C-311/18 (Schrems II), para 105 and the second finding.

is the case for the appropriate safeguards contained in the Article 46 transfer tools, some supplementary measures may be effective in some countries, but not necessarily in others. Those 'supplementary measures' could bring the level of protection of the data transferred up to the EU standard of essential equivalence. Data exporters is responsible to identify and adopt supplementary measures on a case-by-case basis, taking into account the context of the transfer, the third country law and practices and the transfer tool that they are relying on.[105] Several supplementary measures can be applied if needed.

Step 5: Formal procedural steps, if any. If data exporters have identified effective supplementary measures, depending on the Article 46 GDPR transfer tool they are relying on, the required procedural steps may differ according to the EDPB Recommendations.[106]

Step 6: Re-evaluate at appropriate intervals. Exporters must monitor on an ongoing basis the developments of the situation in the third country. If (i) supplementary measures are no longer effective in that third country, or (ii) where those clauses are breached by the importer or is unable to honor the commitments it has taken in the Article 46 GDPR transfer tool, sufficiently sound mechanisms should be put in place to ensure that data exporters can promptly suspend or end data transfers to such third country.[107]

3.2.3. New SCCs

SCCs are the most commonly used of the Article 46 organizational 'appropriate safeguards' and arguably are the dominant mechanism for commercial transborder transfers globally.[108] The adoption of the new SCCs is of importance as it provides 'reinforced clauses' that gives 'more safety and legal certainty to companies for data transfers'[109]. The new SCCs replaces the three sets of SCCs that were adopted under the previous Data Protection Directive[110]. There is a transitional period of three months provided by the

[105] EDPB Recommendations (n 33) 4.
[106] ibid.
[107] ibid 4–5.
[108] Laura Bradford, Mateo Aboy and Kathleen Liddell, 'Standard Contractual Clauses for Cross-Border Transfers of Health Data after *Schrems II*' (2021) 8 Journal of Law and the Biosciences lsab007, 10 <https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsab007/6306998> accessed 22 April 2022.
[109] European Commission (EC), 'European Commission Adopts New Tools for Safe Exchanges of Personal Data' (*EC*, 4 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847> accessed 22 April 2022.
[110] European Commission (EC), 'Standard Contractual Clauses (SCC)' (n 34).

new SCCs, during which companies could continue using the old SCCs. Since 27 September 2021, it is no longer possible for companies entering into new transfer agreements using the old SCCs[111]. Contracts signed before 27 September 2021 that already incorporated the old SCCs will remain valid until 27 December 2022, provided that the processing operations that are the subject matter of the contract remain unchanged[112].

To response to the Schrems II ruling, the new SCCs provide an alternative, multi-layered standard for data protection that encompasses law, technology and organizational commitments[113], which will significantly help companies to comply with the GDPR. Their purpose is to be used in situations where legislation alone is insufficient to protect data subject rights. The European Commission's new draft SCCs support this analysis.[114]

(a) A modular approach and docking clause for more practical implementation

Besides the two previously existing modules of the old SCCs, controllers to controllers - C2C and controllers to processors - C2P, the new SCCs provide two more modules governing data transfer from processors to processors - P2P and processors to controllers - P2C. With the new SCCs, there are separate and free-standing agreements for each type of data transfer where exporters and data importers can now choose the module that best suits their needs in the same agreement.[115] This is the so-called 'modular approach' improved in new SCCs, giving more flexibility to complex processing chains.[116]

There is another innovation in the new SCCs, the new 'docking clause' - Clause 7, which allows an entity that is not a party to the SCCs to be added to them over time as either data exporter or data importer. The supplementary entity might do so by completing the Appendix and signing Annex I.A of the new SCCs (Clause 7(a)). The acceding legal entity thus becomes a party to

[111] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972 OJ L 199. Article 4.1 and 4.2.
[112] ibid. Article 4.3.
[113] Bradford, Aboy and Liddell (n 105) 2.
[114] ibid.
[115] Corrales Compagnucci, Aboy and Minssen (n 29) 8; Ariane Mole, Ruth Boardman and Gabriel Voisin, 'Replacement Standard Contractual Clauses (SCCs): European Commission Publishes Final Text' (*Bird&Bird*, 6 June 2021) <https://www.twobirds.com/en/insights/2021/uk/replacement-standard-contractual-clauses> accessed 24 April 2022.
[116] Corrales Compagnucci, Aboy and Minssen (n 29) 8.

the SCC and has the rights and obligations of a data exporter or data importer under its designation (Clause 7(b)). This provision is optional and allows additional third parties that are not already part of the agreement to enter into the other parties' existing agreement without having to enter into separate contracts[117]. This is believed to provide a more flexible approach to data processing practices, particularly in the context of acquisitions, additional corporate entities and sub-processors.[118]

(b) TIAs to be performed and made available to the supervisory authority on request

As aforementioned, in response to the Schrems II judgment, companies must perform and document a mandatory data privacy impact assessment (DPIA) that should include a TIA and make it available to the competent supervisory authority upon request.[119] The TIAs must take into account: (i) *the specific circumstances of the transfer*, for example, the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; etc. ; (ii) *the laws and practices of the third country of destination* – including those requiring the disclosure of data to public authorities or authorizing access by such authorities – to verify if it could conflict with the SCCs and the GDPR; and (iii) *any relevant contractual, technical or organizational safeguards* put in place to supplement the safeguards under these SCCs.[120]

(c) Stronger commitments on data importers

In response to possible attempts by the third country public authorities to access personal data originating in the EU, the new SCCs offer stronger commitments for the data importers[121]. The data importers have to: (i) notify both data exporters and data subjects that they have received a legally binding request from a public authority for the disclosure of such personal data

[117] ibid 9.
[118] ibid; Martin Braun, Kirk J Nahra and Frédéric Louis, 'European Commission Adopts and Publishes New Standard Contractual Clauses for International Transfers of Personal Data' (7 June 2021) <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data> accessed 24 April 2022.
[119] Corrales Compagnucci, Aboy and Minssen (n 29) 9; Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972 OJ L 199. (n 108) Article 14 of the Annex-SCCs.
[120] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972 OJ L 199. (n 108) Article 14.(b) of the Annex-SCCs.
[121] Mole, Boardman and Voisin (n 112).

(including judicial authorities, under the laws of the country of destination)[122]; (ii) review the legality of the request for disclosure and challenge the request if there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination and international commitments, as well as pursue possibilities of appeal[123]; (iii) seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits and provide the minimum amount of information permissible when responding to a request for disclosure[124]; (iv) document its legal assessment and any challenge to the request for disclosure and make the documentation available to the data exporter or the competent supervisory authority on request[125].

(d) Technical and organizational measures

Annex II of the SCC provides a detailed list of examples of the technical and organizational measures needed to ensure an appropriate level of protection. This list includes technical and organizational measures to ensure the security of data. *Technical measures* include: pseudonymization, encryption, measures for user identification and authorization, measures for the protection of data during transmission, measures for the protection of data during storage, etc. *Organizational measures* include: measures for internal IT and IT security governance and management, Information security management systems (ISMS), Privacy information management systems (PIMS), etc.

Within the limits of this section, it will focus on two very well-known but often confusing techniques: Anonymization and pseudonymization.

> ***Anonymization*** *is a process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party (ISO/TS 25237:2017).*[126]

As mentioned in Article 29 Working Party[127] and under the Recital 26 GDPR, anonymization is a type of data processing in which data must be processed in a way that it can no longer be used to identify a natural person by using "all

[122] See further Clause 15.1 of the new SCCs.
[123] Clause 15.2(a) of the new SCCs.
[124] Clause 15.2(a)(c) of the new SCCs.
[125] Clause 15.2(b) of the new SCCs.
[126] European Network and Information Security Agency., *Pseudonymisation Techniques and Best Practices: Recommendations on Shaping Technology According to Data Protection and Privacy Provisions.* (Publications Office 2019) 10 <https://data.europa.eu/doi/10.2824/247711> accessed 5 May 2022.
[127] Article 29 Data Protection Working Party 0829/14/EN WP216, 'Opinion 05/2014 on Anonymisation Techniques,' 2014.

the means likely reasonably to be used" by either the controller or a third party. Although the GDPR does not directly use the term 'Anonymization', it nevertheless stipulates that the principles of data protection should, therefore, not apply to anonymous information and that the GDPR does not concern the processing of such anonymous information, including for statistical or research purposes.[128]

> ***Pseudonymization*** *is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*[129]

Article 29 Working Party lists the most used pseudonymization techniques, including (i) encryption with secret key, (ii) hash function, (iii) keyed-hash function with stored key, (iv) deterministic encryption or keyed-hash function with deletion of the key, and (v) tokenization[130]. Since pseudonymized data can be traced back to an individual by using a 'code key'[131], whereas anonymized data cannot, it still falls within the scope of the GDPR. This is the key difference that distinguishes the two techniques. It takes extra steps to consider the dataset as anonymized, including removing and generalizing attributes or deleting the original data or at least bringing them to a highly aggregated level[132]. That is why pseudonymization is viewed as a security safeguard under the notion of technical and organizational measures, but it cannot be used to circumvent compliance obligations pursuant to Recitals 26 and 28 GDPR of the GDPR.[133]

3.3. Summary

This chapter firstly went into the provisions of EU law on EU data transfer tools, then dived in the EU data transfer tools that provides by the GDPR Chapter V. This chapter also provided with an overview of the principles of

---

[128] Recital 26 GDPR.
[129] Article 4.5 GDPR.
[130] Article 29 Data Protection Working Party 0829/14/EN WP216, 'Opinion 05/2014 on Anonymisation Techniques,' 2014. (n 124) 20–21.
[131] 'Pseudonymised and Anonymised Data' (*Office of the Data Protection Ombudsman*) <https://tietosuoja.fi/en/pseudonymised-and-anonymised-data> accessed 10 May 2022.
[132] Article 29 Data Protection Working Party, 21.
[133] Christopher F Mondschein and Cosimo Monda, 'The EU's General Data Protection Regulation (GDPR) in a Research Context' in Pieter Kubben, Michel Dumontier and Andre Dekker (eds), *Fundamentals of Clinical Data Science* (Springer International Publishing 2019) 59 <http://link.springer.com/10.1007/978-3-319-99713-1_5> accessed 6 May 2022.

European data protection law regarding the transfers of personal data within the EU and to third countries outside the EU.

Essentially, the transfers of personal data between EU Member States are free and without restrictions. Transfers of data from the EU to third countries outside the EU or to international organizations are only possible if the specific conditions set forth in Chapter V GDPR are met. In particular, it requires that the third countries to which the data is transferred should ensure an adequate level of protection or that data controls or processors must provide appropriate safeguards to ensure an essentially equivalent level of protection to that in the EU. The mechanisms for cross-border data transfers from the EU to third countries outside the EU provided by Chapter V GDPR are analyzed in the post-Schrems II context, in light with the EDPB Recommendations on supplementary measures and the new SCCs.

Chapter 4. Schrems I and II judgments and the aftermath

4.1. Invalidation of the Safe Harbor Decision and the Privacy Shield Decision

To facilitate transborder data flows between the EU and the US, the EC has issued the Safe Harbor Decision and the Privacy Shield Decision. In 2015, the Safe Harbor Decision was found invalid in 2015 by the CJEU in Schrems I. In 2020, the CJEU also invalidated the Privacy Shield Decision in the case of Schrems II by finding that the Privacy Shield Decision did not guarantee satisfactory data protection in accordance with the EU law.

4.1.1. Schrems I

The EU had previously granted a partial adequacy decision for the US under the Data Protection Directive in the form of the Safe Harbor Decision, an adequacy decision, which allowed US-based companies to voluntarily self-certify compliance with certain data privacy standards under the Safe Harbour principles.[134] Max Schrems lodged a complaint with the Irish Data Protection Authority (DPA) asking for the investigation of his personal data transfers from the Facebook's EU headquarters in the EU (based in Ireland) to servers in the US. In his complaint, he argued that the transfer of EU citizens' personal data from the EU to the US under the Safe Harbor Decision did not offer the adequacy protection to EU citizens required by the EU law, given that Facebook had to grant the US National Security Agency access to such data according to the US law and practice[135].

After being rejected by the Irish DPA on the ground that the EU-US data transfer relies on the Commission's binding Safe Harbor Decision, the case was brought to the High Court of Ireland and then was referred to the CJEU for a preliminary ruling. The CJEU confirmed that the adequacy decision shall not prevent the national DPA's powers from examining a person's claim (as enshrined in the Data Protection Directive and the CFR) and considered the validity of the Safe Harbor Decision[136].

---

[134] Liss and others (n 84).

[135] noyb, 'EU-US Data Transfers' (*noyb*, 9 January 2020) <https://noyb.eu/en/project/eu-us-transfers> accessed 3 April 2022.

[136] 'The CJEU's Schrems Ruling on the Safe Harbour Decision' (*European Parliamentary Research Service (EPRS)*, October 2015) 2 <https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/569050/EPRS_ATA(2015)569050_EN.pdf> accessed 8 May 2022.

In the judgment on 6 October 2015, *Schrems I*, the CJEU found the Safe Harbor Decision invalid.[137] Apart from interpreting the term 'adequate level of protection' as requiring the third country to ensure 'level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union'[138], the CJEU found that the EC failed to comply with the requirements laid down in Article 25.6 of the Data Protection Directive as the EC did not find and state in the Safe Harbor Decision that the US in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commit[139]. Therefore, this was a violation of EU privacy law and the fundamental principles enshrined in Articles 7, 8 and 47 of the CFR. [140]

4.1.2. Schrems II

Following the Schrem I judgment, Facebook Ireland and other companies have relied on SCCs to transfer personal data to outside the EU[141]. The EC adopted the Privacy Shield Decision as a replacement for the invalidated Safe Harbour principles.[142] The Privacy Shield framework enables lawful transfer of personal data from the EU to the US, ensuring a strong set of data protection requirements and safeguards[143]. It includes the Privacy Shield list of US-based companies that have been certified to comply with the Privacy Shield principles, to which the EU business can transfer personal data.[144]

In his formulated complaint lodged with the Ireland DPA, Max Schrems argued that the transfer of his personal data from Facebook Ireland to its parent company in the US on the basis of the Commission Decision 2010/87/EU (SCC Decision)[145] failed to protect his fundamental rights under EU law, since the US law requires Facebook Inc. to make the personal data transferred to it available to certain US authorities, such as the National Security Agency (NSA), the Federal Bureau of Investigation (FBI) and the

[137] Schrems II, para 42.
[138] Schrems I, paras 73, 74.
[139] Schrems I, paras 96, 97 and 98.
[140] Corrales Compagnucci, Aboy and Minssen (n 29) 4.
[141] Mildebrath Hendrik, 'The CJEU Judgment in the Schrems II Case' (*European Parliamentary Research Service (EPRS)*, September 2020) 1 <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf> accessed 6 April 2022; Corrales Compagnucci, Aboy and Minssen (n 29) 4.
[142] Liss and others (n 84); Hendrik (n 137).
[143] Hendrik (n 137) 1.
[144] ibid.
[145] 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 (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100) (SCC Decision).

Central Intelligence Agency (CIA). He submitted that, since that data was used in the context of various monitoring program in a manner incompatible with Articles 7, 8 and 47 of the CFR, the SCC Decision could not justify the transfer of that data to the US. Therefore, he asked the Commissioner to prohibit or suspend such transfer of personal data.[146]

When Mr. Schrems's reformulated complaint raised the issue of the validity of the SCC Decision, on 31 May 2016, the Commissioner brought an action before the Irish High Court, relying on the case-law arising from the judgment of Schrems I (para 65). The Irish High Court made the present reference and referred the question on this matter to the CJEU for a preliminary ruling.[147] The Irish High Court referred to a judgment handed down on 3 October 2017, according to which the US authorities' intelligence activities concerning the personal data transferred to the US are based, inter alia, on Section 702 of the Foreign Intelligence Surveillance Act (FISA) and on Executive Order 12333 (E.O. 12333).[148] Section 702 of the FISA permits the Attorney General and the Director of National Intelligence to authorize jointly (following the approval of the US Foreign Intelligence Surveillance Court - FISC) the surveillance of non-US citizens located outside the US to obtain 'foreign intelligence information' for the PRISM and UPSTREAM surveillance program. By this, the US authorities such as the NSA, FBI and CIA have access to personal data of non-US nationals.[149]

In its request for reference preliminary ruling, the referring court also noted that the EU-US data transfer mechanism and the Privacy Shield Decision became relevant to the case, which prompted the CJEU to also rule on the validity of this instrument.[150] In this regard, the CJEU in the Schrems II judgment found that the Privacy Shield did not meet EU data protection standards and was invalidated.[151] In particular, the Court annulled the EU-US Privacy Shield framework and upheld the use of the SCCs[152]. The Court ruled that the US intelligence-gathering laws, failed to comply with the GDPR's principle of proportionality as it did 'not indicate any limitations on the power it confers to implement surveillance programs'.[153] It is also found that the US does not provide an essentially equivalent, and therefore sufficient, level of protection as guaranteed by the GDPR and the CFR[154].

[146] Schrems II, para 55.
[147] Schrems II, para 57.
[148] Schrems II, para 58-60.
[149] Schrems II, para 61-65.
[150] Schrems II, para 66-67.
[151] Schrems II, para 199.
[152] Corrales Compagnucci, Aboy and Minssen (n 29) 5.
[153] Hendrik (n 133); Liss and others (n 85); Schrems II, paras 180.
[154] Schrems II, paras 197-199.

4.1.3. Commentary

The first implication of the Schrems II ruling is that companies can no longer continue to rely on the Privacy Shield Decision as an adequate decision to conduct cross-border data transfers. Continuing to invoke the Privacy Shield Decision as the legal basis for cross-border data transfers could subject companies to a fine of up to 20 million euros or 4 % of their global turnover, pursuant to Article 83.5(c) GDPR.[155] This requires data exporters seeking to export data from the EU to the US or to other countries with the lack of an adequacy decision must put in place another means to provide protections, such as, the SCCs or binding corporate rules (to be discussed in Chapter 5).[156] Even with those developments taken, there is still ambiguity and uncertainty about the steps and legal basis for companies to realize this.

There is a great discussion on the broader implications of the Schrems II ruling for operators. Hendrik Mildebrath in his work points out that there are two views on this.[157] On the one hand, vast majority of most companies can continue to use SCC as only a few companies which are communication service providers concerned by US national security laws. Retailers, manufacturers, health care or pharma companies, or the thousands of companies that use SCCs to export employee' data to headquarters in the US are out of the scope, and they can use SCCs to conduct data transfers to the US.[158] On the other hand, others argue that companies can only use the SCCs for data transfers to the US in case that (i) they are not subject to the respective surveillance law or (ii) they provide for 'additional safeguards'.[159] While the SCCs remain valid following Schrems II, the CJEU underlines the need to ensure that these maintain, in practice, a level of protection that is essentially equivalent to the one guaranteed by the GDPR in light of the CFR of the EU.[160] For this, when considering whether to enter into SCCs, the exporter and the importer are primarily responsible for conducting the TIAs to assess if the countries of recipient offer adequate protection guaranteed within the EU.

---

[155] Hendrik (n 137) 2.
[156] Liss and others (n 84).
[157] Hendrik (n 137) 2.
[158] Omer Tene, 'The Show Must Go On' (*International Association of Privacy Professionals (IAPP)*, 17 July 2020) <https://iapp.org/news/a/the-show-must-go-on/> accessed 13 May 2022.
[159] Hendrik (n 137) 2.
[160] EDPB, 'Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems' (*EDPB*, 17 July 2020) <https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en> accessed 13 May 2022.

Not only for data transfers to the US but also for that of other countries whose benefits do not come from the Privacy Shield, the SCCs might remain for some time the main tool for data transfers and the TIAs will be conducted to assess whether the importer's country ensures essentially equivalent level of protections to that in the EU.[161] If the protections offered in the third country are not enough and the exporter is not able to put in place 'additional measures' to remedy this problem, then the data transfers must cease.[162] This, under the control of the DPAs, may prevent the transfer of data to certain important countries whose legislation provides a lower level of personal data protection than the US regarding the ability to access personal data of public authorities, namely China and Russia.[163]

The CJEU's decision in Schrems II was also criticized for its reasoning in the conclusion regarding the new SCCs as it seems 'weak' and 'betrays a lack of familiarity with the practical implications of using them'[164]. In particular, the Court relied on Recital 109 of the GDPR stating that *"the possibility for the controller … to use standard data protection clauses adopted by the Commission … should [not] prevent [it] … from adding other clauses or additional safeguards'* and that the controller *'should be encouraged to provide additional safeguards … that supplement standard [data] protection clauses"*. It proposed using 'supplementary measures'[165] to protect data under the SCCs but missed the opportunity to specify exactly 'supplementary measures' to compensate for the lack of data protection in the third country[166]. Following Schrems II ruling, the EDPB adopted guidelines on the measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data to fill such gaps.[167] After Schrems II, multinational corporations need to take into account a risk-based approach whereby they need to be ready to perform DPIA and TIA in compliance with the EDPB Recommendations and the new SCC requirements.[168]

4.2. Major implications of Schrems II beyond the EU-US data transfers

---

[161] Theodore Christakis, 'After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe' (*European Law Blog*, 21 July 2020) <https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/> accessed 13 May 2022.
[162] ibid.
[163] ibid.
[164] Christopher Kuner, 'The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation' (*European Law Blog*, 17 July 2020) <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/> accessed 13 May 2022.
[165] Schrems II, para 133.
[166] Corrales Compagnucci, Aboy and Minssen (n 29) 1.
[167] ibid.
[168] ibid 12.

4.2.1. Higher standards of protection for cross-border data transfers

Following Schrems II judgment, the EDPB Recommendations, the new SCCs and the requirements it sets forth therein raised the bar for data protection and security in international data transfers[169]. Both data exporters and data importers must now be more active in ensuring data transfer compliance under the new SCCs, as it places more obligations on them.

For the data importers, as aforementioned[170], they now have stronger commitments, such as notification obligations in case of a legally binding request for disclosure of personal data from a public authority, obligations to review the legality of such request and challenge it if there are reasonable grounds or obligations to document its legal assessment and any challenge to the request for disclosure and make the documentation available to the data exporter or the competent supervisory authority on request, etc.

For data exporters, following the CJEU judgment in Schrems II, there is an explicit obligation for them to assess the adequacy of the level of protection for data transfers to a third country outside the EU, taking into consideration the content of the new SCCs, the specific circumstances of the transfer, as well as the legal regime applicable in the importer's country[171]. The judgment also stresses the importance for the exporter and importer to comply with their information obligations under the new SCCs in relation to change of legislation in the importer's country[172]. The Court states that it is for *"controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, […]"*[173], and that they *"are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned"*[174]. This will require data controllers to become experts in third country law in a way that may be difficult in practice or goes beyond their ability, which also poses a particular question of what about transferring data to third countries that are undemocratic or where the rule of law does not apply.[175] Data exporters must comply with these obligations under the new SCCs, otherwise they are bound by the new SCCs to suspend the transfer or

[169] ibid.
[170] Section 3.2.3.(c), p.28-29.
[171] Section 3.2.2, p.25-26; EDPB, 'Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems' (n 156).
[172] ibid.
[173] Schrems II, para 134.
[174] Schrems II, para 142.
[175] Kuner (n 160).

terminate the SCCs or to notify its competent supervisory authority if it intends to continue transferring data.[176]

4.2.2. The enhanced role of the DPAs and greater uncertainty for multinationals

The Schrems II judgment also put the DPAs under pressure to take enforcement actions. The Court referred to Article 55.1 and Article 57.1(a) of the GDPR on the enforcement task of the DPAs, according to which the task of enforcing that regulation is conferred, in principle, on each supervisory authority on the territory of its own Member State. [177] To ensure the consistent application of the GDPR by the DPAs, the Court also underlines that Article 64.2 GDPR provides for the possibility for a DPA which considers that transfers of data to a third country must, in general, be prohibited, to refer the matter to the EDPB for an opinion, which may adopt a binding decision, in particular where a supervisory authority does not follow the opinion issued (Article 65.1(c) GDPR).[178] The EDPB also takes note of the duties for the competent supervisory authorities to suspend or prohibit a transfer of data to a third country pursuant to the new SCCs, if, (i) in the view of the competent supervisory authorities and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country, and (ii) the protection of the data transferred cannot be ensured by other means, in particular where the controller or a processor has not already itself suspended or put an end to the transfer.[179]

The DPAs in its Strategies for 2022[180] indicates that they will more actively enforce the GDPR with the focus on online tracking and international data transfers. In 2022 so far, the DPAs stay true to their strategy with a list of punishments in several Member States. For instance, on 31 March 2022, Spanish SA imposed a total fine of 700,000 EUR on Orange Espagne for a

---

[176] EDPB, 'Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems' (n 156); 'Schrems II Landmark Ruling: A Detailed Analysis' (*Norton Rose Fulbright*, July 2020) <https://www.nortonrosefulbright.com/en/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis> accessed 13 May 2022.

[177] Schrems II, para 147.

[178] Schrems II, para 147.

[179] EDPB, 'Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems' (n 156).

[180] Sebastião Barros Vale, Gabriela Zanfir-Fortuna and Rob van Eijk, 'Insights into the Future of Data Protection Enforcement: Regulatory Strategies of European Data Protection Authorities for 2021-2022' (*Future of Privacy Forum*, July 2021) <https://fpf.org/wp-content/uploads/2021/07/FPF-Europe-report-DPA-Strategies_-from-2021-and-beyond-3-2-1.pdf> accessed 11 February 2022.

loss of confidentiality related to mobile phone sim card duplicate[181]; On 5 April 2022, the Swedish Authority for Privacy Protection (IMY) issued an administrative fine of SEK 7,500,000 against Klarna Bank AB after an investigation had shown that the company did not comply with several rules in the GDPR[182]; Recently on 4 April 2022, the Danish Supervisory Authority reported Danske Bank to the police and proposed a fine of DKK 10 million (1.3 million EUR) for the infringement of Article 5.2 of the GDPR[183]. This increases pressure on multinational companies to enforce and ensure network security and lawful cross-border data transfers.

The situation after Schrems II left a lot of uncertainties for multinational companies in the legal context of cross-border data transfer activities and put companies in a difficult position in their cross-border data transfer operations. There are not only concerns about the future of other adequacy decisions but also skepticism about the continuous use of the SCCs, the meaning of 'additional safeguards', the use of binding corporate rules, the use of article 49 derogations, as well as codes of conduct and other new options that companies can use as alternatives to transfer personal data to third countries.[184] This will be further discussed in Chapter 5.

4.2.3. The impact in reaching agreement on Privacy Shield 2.0 for the US

The Schrems II ruling also has great implications for international relations between the EU and the US. This caused the US diplomatic officials deep disappointment and suggested possible adverse effects on the US$ 7.1 million transatlantic economic relationship[185]. Given the importance of data flows for economic growth as well as for the post-Covid-19 recovery and pledged to work closely with the EU[186], the EC and the US are continuing negotiations on the Privacy Shield 2.0. After more than a year of negotiations, on 25 March 2022, the EC and the US announce that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic

[181] EDPB, 'Spanish SA Imposes a Fine on Orange Espagne, for a Loss of Confidentiality Related to Mobile Phone Sim Card Duplicate' (*EDPB*, 31 March 2022) <https://edpb.europa.eu/news/national-news/2022/spanish-sa-imposes-fine-orange-espagne-loss-confidentiality-related-mobile_en> accessed 14 May 2022.
[182] 'Administrative Fine against Klarna after Investigation' (*Swedish Authority for Privacy Protection (IMY)*, 31 March 2022) <https://www.imy.se/en/news/administrative-fine-against-klarna-after-investigation/> accessed 14 May 2022.
[183] EDPB, 'Danish SA: Fine Proposed for Danske Bank' (*EDPB*, 11 April 2022) <https://edpb.europa.eu/news/national-news/2022/danish-sa-fine-proposed-danske-bank_en> accessed 14 May 2022.
[184] Christakis (n 157).
[185] Hendrik (n 137) 2.
[186] ibid.

data flows and address the concerns raised by the CJEU in the Schrems II decision of July 2020.[187]

The EC and the US reached an agreement in principle for a Trans-Atlantic Data Privacy Framework that sets out following key principles[188]: (i) Based on the new framework, data will be able to flow freely and safely between the EU and participating US companies; (ii) A new set of rules and binding safeguards to limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security; US intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards; (iii) A new two-tier redress system to investigate and resolve complaints of Europeans on access of data by US Intelligence authorities, which includes a Data Protection Review Court; (iv) Strong obligations for companies processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the US Department of Commerce; and (v) Specific monitoring and review mechanisms.

In the new Trans-Atlantic Data Privacy Framework, the EC acknowledges that there are many benefits of the deal.[189] It provides adequate protection of Europeans' data transferred to the US, addressing the Schrems II ruling of the European Court of Justice. In addition, it will help to ensure safe and secure data flows Trans-Atlantic on durable and reliable legal basis, facilitating competitive digital economy and economic cooperation, as well as enabling continued data flows underpinning 900 billion EUR in cross-border commerce every year. This is an agreement in principle and will now have to be translated into legal documents to form the basis of a draft adequacy decision by the EC to put in place the new Trans-Atlantic Data Privacy Framework.[190]

4.3. Summary

In this chapter, a brief of the invalidation of the Safe Harbor Decision and the Privacy Shield Decision through the CJEU rulings in the Schrems I and Schrems II is presented to highlight the background of the topic at hand. After introducing the CJEU cases of Schrems I and II, this part continues with a commentary on the implications of the cases and the invalidation of the Privacy Shield Decision for cross-border data transfers.

---

[187] European Commission (EC), 'Trans-Atlantic Data Privacy Framework' (*EC*, 25 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 14 May 2022.
[188] ibid.
[189] ibid.
[190] ibid.

Following Schrems II, companies and organizations can no longer continue to rely on the Privacy Shield Decision to transfer data from the EU to the US. Continuing to do so when the Privacy Shield Decision has been disabled risks GDPR violations for companies, which can result in fines of up to 20 million EUR or 4% of their global turnover. Not only that, data transfers to third countries outside the EU other than the US are also affected by this ruling. Although there is much debate surrounding the broader implications of the Schrems II ruling for operators, companies can continue to use the SCCs. However, when considering whether to enter into the new SCCs, they must conduct the TIAs on a case-by-case basis to assess if the countries of recipient offer adequate protection guaranteed within the EU.

The second part of this chapter focuses on analyzing challenges that the EU legal mechanisms on cross-border data transfer in Chapter V of the GDPR pose to the inter-functioning of the internal market following Schrems II judgment. It has major implications beyond the EU-US data transfers. It has implications not only for cross-border data transfer relations between the EU and the US but also beyond the framework of trans-Atlantic data transfers. It not only raises higher standards of protection for cross-border data transfers but also enhances the role of DPAs and increases uncertainty for multinationals in their cross-border data transfer activities on the global scale. Finally, in international relations, the Schrems II ruling also has an impact on the EU and US agreement on Privacy Shield 2.0 for transatlantic data flows.

The CJEU's ruling in *Schrems II* raised the bar for data protection in international data transfers for third countries and required organizations to use alternative transfer mechanisms, such as, the SCCs with 'supplementary measures' to ensure adequate protections or derogations or binding corporate rules, to ensure compliance. Also, it creates a lot of uncertainty about the future of international data transfers and creates many challenges for multinational corporations in compliance. This will be discussed and analyzed in the next chapter, Chapter 5.

Chapter 5. Concluding and analysis

5.1. Difficult position of multinational companies – how to tailor the right response?

Developments of the EU regulatory landscape post-Schrems II showed that companies cannot continue to base on the adequacy decision Privacy Shield conduct trans-Atlantic data transfers. The use of the new SCCs was upheld by the Court. However, the Court clarified that data transfers to a third country based on the new SCCs must ensure a level of protection that is 'essentially equivalent' to the EU protection under the GDPR. In doing so, it is primarily for data exporters, in collaboration with data importers, to conduct a detailed examination of data transfer, on a case-by-case basis, the circumstances of such transfer, the adequacy of protection in the third country where data will be transferred to, and the parties processing the data. This, according to Christopher Kuner, will require data controllers to become *experts in third-country law* in a way that is probably beyond the capabilities of many of them[191], which makes it even more difficult for companies to fulfill their obligations and implement their privacy assessments in practice.

In this regard, the Schrems II ruling more or less created a new process that data exporters must comply with, in order to transfer data across borders not only from the EU to the US, but also to countries other than the EU but not the US. This is partly reflected the so-called Brussels Effect. A new concept i.e. Transfer Impact Assessment - the TIA - was created and applied across all data transfer activities of companies, requiring data importers and exporters to coordinate and ensure compliance. This further emphasizes the importance of the parties involved to comply with Chapter V of the GDPR to conduct cross-border data transfers. Only when they comply with the requirements set forth therein can legitimate data transmission be enabled.

As aforementioned[192], the obligations of data exporters to investigate the level of protection will be even more difficult for data transfers to countries such as major markets China and Russia. This is another difficulty for multinational companies. Since those countries pursue a limited transfers approach, which means that they impose strict requirements on cross-border flows of personal data for companies and organizations, such as conditions for storing and sometimes processing of personal data within the country of

[191] Kuner (n 160).
[192] Chapter 4, Section 4.1.3, p. 36.

origin[193]. Also, legal systems of those countries are considered as offering substantially less guarantees than the US in relation with government access to data[194], or even that their legislation (China) dealing with law enforcement and the security services may be difficult to obtain or non-existent[195]. When transferring data to such a third country, factors related to third country law and applicable practice should be considered and assessed to ensure an equivalent level of protection as provided in the EU. Thus, those markets may not currently have legal options available to exercise and facilitate cross-border data transfers for multinational corporations in such manner.

Non-compliance with the GDPR may risk companies fines and problems arisen from data processing may cause risks towards not only companies but also the individuals having their personal data processed. For the individuals, data privacy risks may cause direct impacts on them, such as, embarrassment, damage to their own reputation, discrimination, loss of confidentiality, identity theft or fraud, etc. For companies, it can also cause damage to reputation of the company, customer abandon, non-compliant costs, harm to internal culture, etc. Taking those into consideration, companies must have their own processes and solutions in place to support the management of data privacy risks, including organizational and technical measures applied in different spheres of operations. Especially, for multinational companies, they must have the system of data privacy risk management in both global and national level, of which in each country of business operations, they must ensure that any additional local legal requirements to data transfers and data privacy risks are also thoughtfully considered.

Cross-border data transfers and GDPR compliance may incur significant operational costs to multinational companies for data protection compliance, including costs for human resources as the cyber security and privacy teams may need to be built to handle data security break or incidents or other legal circumstances where the companies may be at risk of hacker or data leak or incidents; costs for IT systems (infrastructure), data storage solutions (self-built on premises data center or engage on cloud /on premises data server providers) and access management (IT access management). Also, GDPR compliance tools for multinational companies: to be compliant with the GDPR requirements, there is a need of data privacy system to perform data mapping and privacy assessments, as well as to put in place a treatment plan and to archive documentations of all related information about data processed and related GDPR compliant assessments in the companies' digital inventory.

[193] The World Bank (WB) (n 20).
[194] Christakis (n 157).
[195] Kuner (n 160).

This can be done and stored on a cloud server or a data center on-premises. In both cases, it costs companies.

Although companies accept the cost of storage, companies still face the risk that the transfer and storage of personal data is still not done legally. Because of the current situation, major cloud storage or data center service providers are all based in the US, namely Google GCP, Microsoft, etc., which raises concerns about Schrems II ruling that intelligence agencies of the US will continue to be able to intervene and access the data of EU citizens. This is a problem that currently has no solution and causes high risks of non-compliance to companies. Potential solutions to this, either the agreement on an adequacy decision of Privacy Shield 2.0 between the EU and the US or EU data localization, shall be discussed in the next section.

The Schrems II ruling somehow creates work overload for companies, especially multinational corporations with high and frequent demands on cross-border data transfer. Data exporters must now verify the data transfer tools that are in place and choose the right one for them. In addition, they must perform their own risk assessments, i.e., DPIAs and TIAs, to ensure that the level of data protection of the recipient country is 'essentially equivalent' to that afforded in the EU, and then adopt supplementary measures to reduce risk and comply with EU law on data transfers.

Chapter V of the GDPR provides some potential choices as alternatives for multinational companies other than the Privacy Shield Decision and/or the SCCs, such as, **Binding Corporate Rules** - BCRs, approved **Codes of Conduct/Certification**, **Consent and the Derogations as set out in Article** 49 of the GDPR.

Binding Corporate Rules ('BCRs') are one mechanism providing appropriate safeguards for third country data transfers under Article 46.2(b) and 47 of the GDPR. BCRs are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises/multinational companies.[196] BCRs require approval from a competent DPA in the EU according to the mechanism set out in Article 63 of the GDPR[197]. Upon the approval, BRC is legally binding and available only for intra-company transfers. The procedure for BRCs approval is time-consuming and may involve several supervisory authorities since the group applying for approval of its BCRs may have

[196] European Commission (EC), 'Binding Corporate Rules (BCR) - Corporate Rules for Data Transfers within Multinational Companies.' (*EC*) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en> accessed 16 May 2022.
[197] ibid.

entities in more than one Member State[198]. Costly, administratively burdensome and often requires significant organizational changes are some of the drawbacks that make the BRC so limited in practice. Since 25 May 2018, there have been only 30 multinational companies with approved BCRs (9 BCRs of processors and 21 BCRs of controllers).[199]

Codes of Conduct and Certifications. A code of conduct (Article 40 GDPR) is a set of guidelines that contribute to the companies or organizations that have adopted the code applying the GDPR's rules properly and effectively.[200] According to Article 41 of the GDPR, Codes of Conduct shall be approved and monitored by the supervisory authority.[201] The GDPR also provides certification mechanisms in Article 42 with the purpose to demonstrate compliance with the GDPR obligations of data controllers and processors regarding their processing of personal data. Certifications provided in the GDPR is voluntary and available via a transparent process (Article 42.3). It is to be issued by an accredited certification body or by a competent supervisory authority (Article 42.5). While the GDPR introduces the possibility of certifications and codes of conduct as mechanisms to enable cross-border transfer, they have limited availability. The first approved transnational codes of conduct under the GDPR were in May 2021 for the EU Cloud Code of Conduct[202]. In February 2022, the EDPB adopted its opinion on the GDPR-CARPA certification scheme submitted to the Board by the Luxembourg Supervisory Authority (SA)[203].

Consent or Necessity. Derogations under Article 49 are exemptions from the general principle that personal data may only be transferred to third countries outside the EU if the third country ensure that they can provide an essentially

---

[198] ibid.

[199] 'Approved Binding Corporate Rules' (*EDPB*) <https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en> accessed 16 May 2022; See also a list of pre-GDPR BCR approved before 25 May 2018 here: 'Pre-GDPR BCRs Overview List' (*EDPB*) <https://edpb.europa.eu/our-work-tools/our-documents/other/pre-gdpr-bcrs-overview-list-0_en> accessed 16 May 2022.

[200] 'Codes of Conduct and Certification' (*Swedish Authority for Privacy Protection (IMY)*, 18 May 2021) <https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/codes-of-conduct-and-certification/> accessed 16 May 2022.

[201] ibid.

[202] ShanShan Pa, 'Code of Conduct: An Effective Tool for GDPR Compliance' (*ISACA*, 18 January 2022) <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/code-of-conduct-an-effective-tool-for-gdpr-compliance> accessed 16 May 2022; EDPB, 'EDPB Adopts Opinions on First Transnational Codes of Conduct, Statement on Data Governance Act, Recommendations on the Legal Basis for the Storage of Credit Card Data.' (*EDPB_Press Release*, 20 May 2021) <https://edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act_en> accessed 16 May 2022.

[203] EDPB, 'EDPB Adopts First Opinion on Certification Criteria' (*EDPB*, 2 February 2022) <https://edpb.europa.eu/news/news/2022/edpb-adopts-first-opinion-certification-criteria_en> accessed 17 May 2022.

equivalent level of protection afforded within the EU.[204] Article 29 Working Party draft guidelines on Article 49 GDPR derogations in the context of transfers of personal data to third countries provides specific interpretation of the provision of Article 49, including consent and transfer necessity as two types of 'derogations': consent and necessity. Data exporters should first endeavor possibilities to frame the transfer with one of the mechanisms included in Articles 45 and 46 GDPR, and only in their absence use the derogations provided in Article 49.1.[205] The availability of a derogation requires a careful and close assessment as it is applicable only in limited circumstances, as an exception rather than the norm.[206]

Conclusion: What should multinational companies do now? In practice, companies must now assess all their data transfer activities on a case-by-case basis, both their trans-Atlantic and global transfers, in light of the Schrems II ruling. For those transfers to the US on the basis of the Privacy Shield, companies need to use other alternatives to enable it, taking to account of the existing privacy principles those underlying the Privacy Shield framework, which was indicated in the US Federal Trade Commission statement[207]. The alternative legal basis that companies can consider in addition to **the new SCCs** may include **the BCRs**, which must be approved on a company-by-company basis by the DPAs, **Codes of Conduct and Certifications**, those are subject to limitations due to the procedures to get it approved. There is also **Consent and other Derogations** outlined under Article 49 of the GDPR that can be used as an option. However, the derogations should be relied on in limited circumstances only.

5.2. EU's response: Towards Data Localization?

In relation to the EU-US Trans-Atlantic data transfers, the first adequacy decision of Safe Harbor Decision was invalidated by the CJEU Schrems I judgment because the US law grants US intelligence agencies the access to EU personal data, which was a violation of EU privacy law and the fundamental principles enshrined in Articles 7, 8 and 47 of the CFR. Privacy Shield Decision was then adopted as the replacement of the Safe Harbor Decision to provide similar system to facilitate data flows cross-Atlantic. The second EU-US adequacy decision Privacy Shield Decision later was declared invalid in 2020 by the CJEU Schrems II judgment. The CJEU in Schrems II

[204] Article 29 Working Party Guidelines on Article 49 of Regulation 2016/679 Adopted on 6 February 2018.
[205] ibid.
[206] 'Schrems II Landmark Ruling: A Detailed Analysis' (n 172).
[207] The US Federal Trade Commission (FTC), 'Privacy Shield' (*FTC*, 21 July 2020) <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield> accessed 13 May 2022.

ruled that this regulation could not provide an essentially equivalent level of protection as guaranteed in the EU law. Again, the reason for this was the interference by US intelligence agencies under the US intelligence-gathering law. Since then, cross-border data transfer activities from the EU to the US became problematic for EU companies.

In January and February 2022, respectively, Google Analytics set-up was found unlawful in Austria and France as the Austrian DPA (DSB)[208] and French DPA (CNIL)[209] ruled that the use of Google Analytics violated the GDPR. Thus, companies deploying Google Analytics technologies on their websites were found in violation of the GDPR. This exposes companies with Google Analytics technology implemented in their digital products to the risk that those products could not be deployed in Austria and France, i.e. the markets affected by the DPAs' Google Analytics decisions. Failure to do so may result in them being found in violation of the GDPR and subject to fines by the respective DPAs. For the time being, this risk is limited to the EU markets and currently has no effective measures available to eliminate it. For the long term, according to Max Schrems, there seems to be two options: Either the US adapts baseline protections for foreigners to support their tech industry, or US providers will have to host foreign data outside of the US.[210]

On 25 March 2022, the EC announced that an agreement in principle for a Trans-Atlantic Data Privacy Framework was reached between the EU and the US, which would foster trans-Atlantic data flows and address the concerns raised by the CJEU in the Schrems II decision of July 2020. On 6 April 2022, following the EU Commission - US Joint Statement on Trans-Atlantic Data Privacy Framework, the EDPB adopted a statement with respect to the new adequacy decision, the US Trans-Atlantic Data Privacy Framework. In its statement, the EDPB adopted that:

> *The commitment of the US highest authorities to establish 'unprecedented' measures to protect the privacy and personal data of individuals in the European Economic Area (EEA individuals) when*

[208] noyb, 'Austrian DSB: EU-US Data Transfers to Google Analytics Illegal' (*noyb*, 13 January 2022) <https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal> accessed 15 May 2022; DSB, 'DSB (Austria) Decision' <https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk.pdf> accessed 15 May 2022.

[209] French Data Protection Authority (the "CNIL"), 'Use of Google Analytics and Data Transfers to the United States: The CNIL Orders a Website Manager/Operator to Comply' (*CNIL*, 10 February 2022) <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply> accessed 8 February 2022.

[210] noyb (n 204).

their data are transferred to the US is a positive first step in the right direction.[211]

The EDPB will examine how this political agreement translates into concrete legal proposals to address the concerns raised by the CJEU in order to provide legal certainty to EEA individuals and exporters of data.[212]

At this stage, the EDPB also went on to state that this agreement did not constitute a legal framework on which data exporters could base their data transfers to the US, and data exporters had to, therefore, continue taking the actions required to comply with the caselaw of the CJEU, and in particular its Schrems II decision.[213] This principle agreement will now have to be translated into legal documents to form the basis of a draft adequacy decision by the EC to put in place the new Trans-Atlantic Data Privacy Framework. This process certainly takes time. In the meantime, transferring data from the EU to the US requires specific TIAs to review the full range of safeguards to include legal measures, such as the use of SCCs, technical and organizational measures.

In this regard, EDPB Chair Andrea Jelinek said the proposed Trans-Atlantic Data Privacy Framework and the "commitment of the US highest authorities to establish 'unprecedented' measures" is "a positive first step".[214] However, given the fundamental legal clash between EU privacy rights and US surveillance overreach that has been brought up in the judgments of Schrems I and II, Privacy Shield 2.0 may not be a stable and ultimate legal tool to deal with cross-border data transfers between the EU and the US. Commentators and privacy experts reacted very critically immediately after the EU Commission - US Joint Statement on Trans-Atlantic Data Privacy Framework made on 25 March 2022 by the EU Commission. In particular, *noyb* and activist Max Schrems said the lack of details was troubling and that if the US was only offering executive reassurances instead of changing its surveillance laws, he would not hesitate to go to court again and 'play the same game a third time now'.[215]

---

[211] 'Statement 01/2022 on the Announcement of an Agreement in Principle on a New Trans-Atlantic Data Privacy Framework Adopted on 6 April 2022.' (*EDPB*, 6 April 2022) <https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf> accessed 15 May 2022.
[212] ibid.
[213] ibid.
[214] IAPP, 'EDPB Releases Statement on EU-US Data Flows Political Agreement' (*IAPP*, 7 April 2022) <https://iapp.org/news/a/edpb-applauds-eu-u-s-agreement-on-data-flows-further-review-coming/> accessed 15 May 2022.
[215] Francesco Guarascio and Foo Yun Chee, 'EU-U.S. Data Transfer Deal Cheers Business, but Worries Privacy Activists' (*Reuters*, 25 March 2022)

> *"The final text will need more time, once this arrives we will analyze it in depth, together with our U.S. legal experts. If it is not in line with EU law, we or another group will likely challenge it,"* said Max Schrems in a statement.[216]

Although reaching a framework agreement between the EU and the US on trans-Atlantic data transfer has received positive political reactions[217], there are still concerns related to the third adequacy decision between the EU and the US. This concern is mainly about the vague principles laid out in the agreement and whether the EU and the US can achieve new Privacy Shield on this basis.[218] The potential Privacy Shield 2.0 would clearly provide an opportunity for the EU and US to clarify and strengthen the protections for data privacy and provide greater legal certainty for trans-Atlantic commerce. This requires privacy experts and lawmakers (mainly from the US side) to make significantly possible changes in US national security legislation.[219] Without doing so, the core of the whole matter in both the Schrems I and Schrems II judgments will remain unchanged. This is the most striking issue as Max Schrems is likely, as mentioned in his statement, to continue lodging the complaint that leads to another Schrems case to dismiss the Privacy Shield 2.0, Schrems III.

Examining the alternatives for transferring personal data to third countries outside the EU post-Schrems II reveals that this process is quite difficult. In practical, the end result may be the pressure on data localization for EU companies and US-based IT service suppliers. When implementing a TIA, companies will be required to evaluate the data transfer practices and laws of the third country to which the data is transferred, and to identify and apply technical and organizational measures to ensure the level of protection is essentially equivalent to that of the EU data protection. In this process, risks often arise if, during the entire lifecycle of a digital product in which a company conducts cross-border data transfers, personal data is processed in a third country (many of the most at-risk are the US, Russia and China), for which these third countries do not have adequacy decisions or do not guarantee an appropriate level of protection. In addition, the risk of non-

---

<https://www.reuters.com/legal/litigation/eu-us-reach-preliminary-deal-avoid-disruption-data-flows-2022-03-25/> accessed 15 May 2022.

[216] noyb, '"Privacy Shield 2.0"? - First Reaction by Max Schrems' (*noyb*, 25 March 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 15 May 2022.

[217] Bart Van den Brande, '"Agreement" on a New Privacy Shield: Schrems III in the Making?' (*Sirius Legal*) <https://siriuslegaladvocaten.be/en/blogs/agreement-new-privacy-shield-or-schremsiii/> accessed 16 May 2022.

[218] ibid.

[219] ibid.

compliance is also red-flagged if personal data is stored in a data center outside of the EU, specifically in the US; or hosted on a cloud service provided by a US-based company. As mentioned in the previous section, the transfer of personal data to the US or the provision of cloud storage services by a US-based company to store/host the personal data of EU citizens may be subject to compliance with US intelligence laws, and therefore the personal information of EU citizens may be accessed, which violates EU data protection law and the CFR.

In light of the Schrems II ruling on EU-US data transfer framework, many cloud storage service providers have had updates regarding EU businesses. Specifically, Google had an update on Google Cloud's commitments to EU businesses, according to which Google offers customer-managed encryption and data localization for a growing list of key products and collaborating with local partners to provide the highest levels of sovereignty. For Google Cloud Platform (GCP), companies now can store their data in their choice of EU Google Cloud region(s), which is ensured that only EU persons – located in the EU – have access to the data. Google also provides cryptographic control for data access, including customer-managed encryption keys.[220] However, this is not a solution to the issue at hand. Since Google is a US-based company, even if the primary storage location is within the EU, the US is still one of the locations where data is likely to be transferred, if a FISA request is made.

Schrems II complicates data transfers from the EU to much of the rest of the world, leading to the practical effect of Schrems II of putting pressure on companies to keep data inside the EU.[221] To comply with the GDPR requirements on data transfer outside the EU, companies must choose EU alternatives to replace the US-based ones for most the digital products for example cloud services, web analytics, etc. Many commentators have suggested data localization as one solution to the problem. They called it the emergence of a "soft data localization" mandate in the EU based on Schrems II, which refers to 'a legal regime that puts pressure on companies to localize, not by directly requiring localization of data or processes, but by making alternatives legally risky and thus potentially unwise'[222].

[220] Marc Crandall and Nathaly Rey, 'An Update on Google Cloud's Commitments to E.U. Businesses in Light of the New E.U.-U.S. Data Transfer Framework' (*Google Cloud*, 29 March 2022) <https://cloud.google.com/blog/products/identity-security/how-google-cloud-helps-eu-companies-under-new-data-transfer-rules> accessed 16 May 2022.
[221] Anupam Chander, 'Is Data Localization a Solution for Schrems II?' (2020) 23 Journal of International Economic Law 771, 2 <https://academic.oup.com/jiel/article/23/3/771/5909035> accessed 16 May 2022.
[222] ibid.

Data localization will help EU companies reduce risk and ensure GDPR compliance. Simply because data localization seems to avoid the problems that the decision raises: if there is no data transfer outside the EU, then there is no need to take the risk that the transfer will be found invalid by a data protection authority or a court.[223] However, this option is considered expensive in terms of operational costs and given the nature of the problem, data localization does not solve US surveillance issue.[224] The Schrems II ruling highlighted irreconcilable differences between the EU and US approaches to data privacy and the original issue to be forced to walk back is foundational aspects of the US legal system about surveillance programs.[225]

What needs to be done at the EU level? We may need to look forwards to further legislation developments from the EU: (i) legislative change towards a solution that further strengthens the accountability and transparency of organizations or (ii) policy change in strengthening technical innovation and infrastructure development to make the EU ready to realize data localization to meet the actual needs of businesses. At this moment, what multinational companies can do to remain compliant with the EU law when transferring personal data outside the EU is that they can keep using the new SCCs and the BRCs (or otherwise the alternative mechanisms that are practically available). While doing so, they need to perform their own DPIA and TIA assessments following the EDPB Recommendations and the GDPR. An effective privacy assessment process will allow companies to identify and mitigate the risks of data transfers. Mitigating and lowering privacy risks of cross-border data transfers will help companies reduce associated costs and damage to their reputation that they could otherwise face. Another important step for companies is to document all relevant agreements, technical documents, dataflow diagrams, etc. to prepare themselves for any request from the competent authorities. Taking those steps will help companies comply with GDPR and reduce risks in their security and privacy practices, as well as achieve a higher level of trust from customers, which is one of the main goals of any business.

[223] ibid 7.
[224] ibid 8.
[225] H Jacqueline Brehmer, 'Data Localization: The Unintended Consequences of Privacy Litigation' (2018) 67 American University Law Review <https://aulawreview.org/blog/data-localization-the-unintended-consequences-of-privacy-litigatio/#_ftn188> accessed 17 May 2022.

Bibliography

Case law

Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd [2020] ECLI:EU:C:2020:559.

Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

Legislation and documents from institutions

Article 29 Data Protection Working Party 0829/14/EN WP216, 'Opinion 05/2014 on Anonymisation Techniques,' 2014.

Article 29 Working Party Guidelines on Article 49 of Regulation 2016/679 Adopted on 6 February 2018.

Charter of Fundamental Rights of the European Union (adopted 2 October 2000, entered into force 7 December 2000) OJ C 326/291 (CFR).

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 (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100) (SCC Decision).

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 [2016] OJ L207/1 (Privacy Shield Decision).

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972 OJ L 199.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, a Digital Single Market Strategy for Europe, COM/2015/0192 final.

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU).

Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation, OJ 1994 L 1.

Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L [1995] 281/31.

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 4.5.2016 (Law Enforcement Directive)

EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0. Adopted on 18 June 2021 (the EDPB Recommendations).

European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) ETS 5 (ECHR).

Modernized Convention for the Protection of Individuals with regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session of the Committee of Ministers (Elsinore, 18 May 2018) (Convention 108).

Regulation 2016/679 of the European Parliament and of the Council of April 27, 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 [2016] 119/1 (hereinafter the GDPR).

Literature

Bradford A, The Brussels Effect: How the European Union Rules the World (1st edn, Oxford University Press 2020) <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190088583.001.0001/oso-9780190088583> accessed 17 April 2022

Craig P and De Búrca G, EU Law: Text, Cases, and Materials (Sixth edition, Oxford University Press 2015)

Kuner C, Transborder Data Flows and Data Privacy Law (Oxford University Press 2013) <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199674619.001.0001/acprof-9780199674619> accessed 10 April 2022

—— (eds), The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198826491.001.0001/isbn-9780198826491> accessed 13 March 2022

Moerel EML, Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers (1st ed, Oxford University Press 2012)

Pila J and Torremans P, European Intellectual Property Law (2nd edition, Oxford University Press 2019)

Journal Articles

Bradford L, Aboy M and Liddell K, 'Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II' (2021) 8 Journal of Law and the Biosciences lsab007 <https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsab007/6306998> accessed 22 April 2022

Brehmer HJ, 'Data Localization: The Unintended Consequences of Privacy Litigation' (2018) 67 American University Law Review <https://aulawreview.org/blog/data-localization-the-unintended-consequences-of-privacy-litigatio/#_ftn188> accessed 17 May 2022

——, 'Data Localization: The Unintended Consequences of Privacy Litigation' (American University Law Review (Volume 67; J.D), May 2018) <https://aulawreview.org/blog/data-localization-the-unintended-consequences-of-privacy-litigatio/#_ftn188> accessed 17 May 2022

Breitbarth P, 'A Risk-Based Approach to International Data Transfers' (2021) 7 European Data Protection Law Review 539 <http://edpl.lexxion.eu/article/EDPL/2021/4/9> accessed 6 March 2022

Burri and Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 Journal of Information Policy 479 <http://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0479> accessed 19 April 2022

Chander A, 'Is Data Localization a Solution for Schrems II?' (2020) 23 Journal of International Economic Law 771 <https://academic.oup.com/jiel/article/23/3/771/5909035> accessed 16 May 2022

Corrales Compagnucci M, Aboy M and Minssen T, 'Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3951085> accessed 6 March 2022

European Network and Information Security Agency., Pseudonymisation Techniques and Best Practices: Recommendations on Shaping Technology According to Data Protection and Privacy Provisions. (Publications Office 2019) <https://data.europa.eu/doi/10.2824/247711> accessed 5 May 2022

European Union Agency for Fundamental Rights and others, Handbook on European Data Protection Law : 2018 Edition (Publications Office 2018) <https://data.europa.eu/doi/10.2811/343461> accessed 17 April 2022

Gestrin, Michael V JS, 'The Digital Economy, Multinational Enterprises and International Investment Policy' [2018] OECD <http://www.oecd.org/investment/the-digital-economy-mnes-and-international-investment-policy.htm> accessed 8 March 2022

Hijmans H, 'The Mandate of the EU Under Article 16 TFEU and the Perspectives of Legitimacy and Effectiveness' in Hielke Hijmans, The European Union as Guardian of Internet Privacy, vol 31 (Springer International Publishing 2016) <http://link.springer.com/10.1007/978-3-319-34090-6_4> accessed 19 April 2022

Hoecke MV, Methodologies of Legal Research: What Kind of Method for What Kind of Discipline? (Hart Publishing 2011)

<http://www.bloomsburycollections.com/book/methodologies-of-legal-research-what-kind-of-method-for-what-kind-of-discipline> accessed 14 March 2022

Hoofnagle CJ, van der Sloot B and Borgesius FZ, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law 65 <https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501> accessed 26 March 2022

Liss J and others, 'Demystifying Schrems II for the Cross-Border Transfer of Clinical Research Data' (2021) 8 Journal of Law and the Biosciences lsab032 <https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsab032/6407729> accessed 29 March 2022

Mondschein CF and Monda C, 'The EU's General Data Protection Regulation (GDPR) in a Research Context' in Pieter Kubben, Michel Dumontier and Andre Dekker (eds), Fundamentals of Clinical Data Science (Springer International Publishing 2019) <http://link.springer.com/10.1007/978-3-319-99713-1_5> accessed 6 May 2022

Murphy MH, 'ASSESSING THE IMPLICATIONS OF SCHREMS II FOR EU–US DATA FLOW' (2022) 71 International and Comparative Law Quarterly 245 <https://www.cambridge.org/core/product/identifier/S0020589321000348/type/journal_article> accessed 28 March 2022

Smits JM, 'What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' [2015] SSRN Electronic Journal <http://www.ssrn.com/abstract=2644088> accessed 14 March 2022

'Pseudonymised and Anonymised Data' (Office of the Data Protection Ombudsman) <https://tietosuoja.fi/en/pseudonymised-and-anonymised-data> accessed 10 May 2022

van Gestel R and Micklitz H-W, 'Why Methods Matter in European Legal Scholarship: Methods in European Legal Scholarship' (2014) 20 European Law Journal 292 <https://onlinelibrary.wiley.com/doi/10.1111/eulj.12049> accessed 14 March 2022

Other electronic sources

‘Administrative Fine against Klarna after Investigation’ (Swedish Authority for Privacy Protection (IMY), 31 March 2022) <https://www.imy.se/en/news/administrative-fine-against-klarna-after-investigation/> accessed 14 May 2022

‘Approved Binding Corporate Rules’ (EDPB) <https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en> accessed 16 May 2022

Archick K and Fefer RF, ‘U.S.-EU Privacy Shield and Transatlantic Data Flows’ (Congressional Research Service (CRS) 2021) R46917 <https://crsreports.congress.gov/product/pdf/R/R46917#:~:text=Since%20the%20media%20leaks%20of,Privacy%20Shield%20Framework%2C%20in%202020.> accessed 22 March 2022

Barros Vale S, Zanfir-Fortuna G and van Eijk R, ‘Insights into the Future of Data Protection Enforcement: Regulatory Strategies of European Data Protection Authorities for 2021-2022’ (Future of Privacy Forum, July 2021) <https://fpf.org/wp-content/uploads/2021/07/FPF-Europe-report-DPA-Strategies_-from-2021-and-beyond-3-2-1.pdf> accessed 11 February 2022

Braun M, Nahra KJ and Louis F, ‘European Commission Adopts and Publishes New Standard Contractual Clauses for International Transfers of Personal Data’ (7 June 2021) <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data> accessed 24 April 2022

Christakis T, ‘After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe’ (European Law Blog, 21 July 2020) <https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/> accessed 13 May 2022

‘Codes of Conduct and Certification’ (Swedish Authority for Privacy Protection (IMY), 18 May 2021) <https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/codes-of-conduct-and-certification/> accessed 16 May 2022

Crandall M and Rey N, ‘An Update on Google Cloud’s Commitments to E.U. Businesses in Light of the New E.U.-U.S. Data Transfer Framework’ (Google Cloud, 29 March 2022) <https://cloud.google.com/blog/products/identity-

security/how-google-cloud-helps-eu-companies-under-new-data-transfer-rules> accessed 16 May 2022

DSB, 'DSB (Austria) Decision' <https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk.pdf> accessed 15 May 2022

EDPB, 'Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems' (EDPB, 17 July 2020) <https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en> accessed 13 May 2022

——, 'EDPB Adopts Opinions on First Transnational Codes of Conduct, Statement on Data Governance Act, Recommendations on the Legal Basis for the Storage of Credit Card Data.' (EDPB_Press Release, 20 May 2021) <https://edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act_en> accessed 16 May 2022

——, 'EDPB Adopts Final Version of Recommendations on Supplementary Measures, Letter to EU Institutions on the Privacy and Data Protection Aspects of a Possible Digital Euro, and Designates Three EDPB Members to the ETIAS Fundamental Rights Guidance Board' (EDPB_Press Release, 21 June 2021) <https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en> accessed 20 April 2022

——, 'EDPB Adopts First Opinion on Certification Criteria' (EDPB, 2 February 2022) <https://edpb.europa.eu/news/news/2022/edpb-adopts-first-opinion-certification-criteria_en> accessed 17 May 2022

——, 'Spanish SA Imposes a Fine on Orange Espagne, for a Loss of Confidentiality Related to Mobile Phone Sim Card Duplicate' (EDPB, 31 March 2022) <https://edpb.europa.eu/news/national-news/2022/spanish-sa-imposes-fine-orange-espagne-loss-confidentiality-related-mobile_en> accessed 14 May 2022

——, 'Danish SA: Fine Proposed for Danske Bank' (EDPB, 11 April 2022) <https://edpb.europa.eu/news/national-news/2022/danish-sa-fine-proposed-danske-bank_en> accessed 14 May 2022

European Commission (EC), ‘European Commission Adopts New Tools for Safe Exchanges of Personal Data’ (EC, 4 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847> accessed 22 April 2022

——, ‘Trans-Atlantic Data Privacy Framework’ (EC, 25 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 14 May 2022

——, ‘Adequacy Decisions’ (EC) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 28 March 2022

——, ‘Binding Corporate Rules (BCR) - Corporate Rules for Data Transfers within Multinational Companies.’ (EC) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en> accessed 16 May 2022

——, ‘Data Protection in the EU’ (EC) <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en> accessed 26 March 2022

——, ‘Rules on International Data Transfers’ (EC) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en> accessed 10 February 2022

——, ‘Standard Contractual Clauses (SCC)’ (EC) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> accessed 22 April 2022

——, ‘Types of EU Law’ (EC) <https://ec.europa.eu/info/law/law-making-process/types-eu-law_en#:~:text=Treaties%20are%20the%20starting%20point,%2C%20decisions%2C%20recommendations%20and%20opinions.> accessed 22 March 2022

——, ‘What Rules Apply If My Organisation Transfers Data Outside the EU?’ (EC) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en> accessed 20 April 2022

European Data Protection Supervisor (EDPS), 'Data Protection' (EDPS) <https://edps.europa.eu/data-protection/data-protection_en> accessed 22 March 2022

French Data Protection Authority (the "CNIL"), 'Use of Google Analytics and Data Transfers to the United States: The CNIL Orders a Website Manager/Operator to Comply' (CNIL, 10 February 2022) <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply> accessed 8 February 2022

Granmar C, 'E-Commerce and the EU Data Protection Regulation' <https://www.diva-portal.org/smash/get/diva2:1278665/FULLTEXT01.pdf> accessed 20 March 2022

Guarascio F and Chee FY, 'EU-U.S. Data Transfer Deal Cheers Business, but Worries Privacy Activists' (Reuters, 25 March 2022) <https://www.reuters.com/legal/litigation/eu-us-reach-preliminary-deal-avoid-disruption-data-flows-2022-03-25/> accessed 15 May 2022

Hendrik M, 'The CJEU Judgment in the Schrems II Case' (European Parliamentary Research Service (EPRS), September 2020) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf> accessed 6 April 2022

IAPP, 'EDPB Releases Statement on EU-US Data Flows Political Agreement' (IAPP, 7 April 2022) <https://iapp.org/news/a/edpb-applauds-eu-u-s-agreement-on-data-flows-further-review-coming/> accessed 15 May 2022

Julisch K and Widmer F, 'GDPR Update: The Future of International Data Transfers' (Deloitte) <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-the-future-of-international-data-transfer.html> accessed 12 February 2022

——, 'The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation' (European Law Blog, 17 July 2020) <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/> accessed 13 May 2022

Luisi M, ‘GDPR as a Global Standards? Brussels’ Instrument of Policy Diffusion’ (9 April 2022) <https://www.e-ir.info/2022/04/09/gdpr-as-a-global-standards-brussels-instrument-of-policy-diffusion/> accessed 14 April 2022

Mole A, Boardman R and Voisin G, ‘Replacement Standard Contractual Clauses (SCCs): European Commission Publishes Final Text’ (Bird&Bird, 6 June 2021) <https://www.twobirds.com/en/insights/2021/uk/replacement-standard-contractual-clauses> accessed 24 April 2022

noyb, ‘EU-US Data Transfers’ (noyb, 9 January 2020) <https://noyb.eu/en/project/eu-us-transfers> accessed 3 April 2022

——, ‘Austrian DSB: EU-US Data Transfers to Google Analytics Illegal’ (noyb, 13 January 2022) <https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal> accessed 15 May 2022

——, ‘“Privacy Shield 2.0”? - First Reaction by Max Schrems’ (noyb, 25 March 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 15 May 2022

OECD, ‘Personal Data Protection at the OECD’ (Organisation for Economic Co-operation and Development (OECD)) <https://www.oecd.org/general/data-protection.htm> accessed 12 April 2022

Pa S, ‘Code of Conduct: An Effective Tool for GDPR Compliance’ (ISACA, 18 January 2022) <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/code-of-conduct-an-effective-tool-for-gdpr-compliance> accessed 16 May 2022

‘Pre-GDPR BCRs Overview List’ (EDPB) <https://edpb.europa.eu/our-work-tools/our-documents/other/pre-gdpr-bcrs-overview-list-0_en> accessed 16 May 2022

Renzo Marchini, ‘Data Transfers within a Multinational Group Safely Navigating EU Data Protection Rules’ (Dechert LLP, May 2013) <https://www.lexology.com/library/detail.aspx?g=2b2f345f-a5fa-4001-98e3-f189a5441644> accessed 10 February 2022

‘Schrems II Landmark Ruling: A Detailed Analysis’ (Norton Rose Fulbright, July 2020)

<https://www.nortonrosefulbright.com/en/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis> accessed 13 May 2022

'Statement 01/2022 on the Announcement of an Agreement in Principle on a New Trans-Atlantic Data Privacy Framework Adopted on 6 April 2022.' (EDPB, 6 April 2022) <https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf> accessed 15 May 2022

Tene O, 'The Show Must Go On' (International Association of Privacy Professionals (IAPP), 17 July 2020) <https://iapp.org/news/a/the-show-must-go-on/> accessed 13 May 2022

'The CJEU's Schrems Ruling on the Safe Harbour Decision' (European Parliamentary Research Service (EPRS), October 2015) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/569050/EPRS_ATA(2015)569050_EN.pdf> accessed 8 May 2022

'The European Economic Area (EEA) Includes All EU Countries and Non-EU Countries Iceland, Liechtenstein and Norway'

'The Internal Market: General Principles' (Fact Sheets on the European Union - 2022) <https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.1.1.pdf> accessed 4 May 2022

The US Federal Trade Commission (FTC), 'Privacy Shield' (FTC, 21 July 2020) <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield> accessed 13 May 2022

The World Bank (WB), 'Data for Better Lives - Crossing Borders' (The World Bank 2021) <https://wdr2021.worldbank.org/stories/crossing-borders/> accessed 13 March 2022

Van den Brande B, '"Agreement" on a New Privacy Shield: Schrems III in the Making?' (Sirius Legal) <https://siriuslegaladvocaten.be/en/blogs/agreement-new-privacy-shield-or-schremsiii/> accessed 16 May 2022

Voronova S and Nichols A, 'Understanding EU Data Protection Policy' (European Parliamentary Research Service (EPRS), May 2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf> accessed 5 May 2022