September 15, 2022

Transatlantic Data Transfer Compliance

W. Gregory Voss

ARTICLE

TRANSATLANTIC DATA TRANSFER COMPLIANCE

W. GREGORY VOSS†

ABSTRACT

Data play a central role in the economy today. Nonetheless, the main trading partner of the United States—the European Union—places restrictions on cross-border transfers of personal data exported from the European Union. Destination countries must benefit from a decision by the European Commission that their data protection practice is "adequate" to import data, or transfer tools must be used to further protect those data. The United States does not benefit from such a decision and an arrangement that previously allowed data to continue to flow to the United States—the Privacy Shield—was invalidated by the Court of Justice of the European Union in 2020 in a case that is known as Schrems II.

*This study focuses on EU-U.S. personal data transfers. It provides a holistic view of the legal parameters involved in transatlantic data transfer compliance post-*Schrems II*, relevant developments past and future, and potential compliance actions, supplemented with relevant guidance and an analysis of enforcement actions. Such compliance is considered the most difficult task of privacy professionals today. The aim is to give a fuller understanding in this context of the EU General Data Protection Regulation (GDPR), which sets out the cross-border data transfer restriction, with a view to potential pathways to navigate those challenges.*

Following the Introduction, this study dives into both the cross-border transfer restriction contained in the GDPR, and into the Schrems II *ruling. EU-U.S. negotiations to try to build a replacement for the Privacy Shield are discussed. A new 2021 version of the standard contractual clauses transfer tool, used to allow data exports, is analyzed. In addition, the requirement to respect the essence of fundamental rights and freedoms set out in the* Schrems II *judgment is explained. Supplemental measures to ensure data protection and to allow transfers to jurisdictions with problematic legislation, such as the United States (with its surveillance laws), are detailed. Furthermore, European Economic Area data protection enforcement action in the domain of cross-border transfers is studied, including a recent case relating to the use of the popular Google*

† Associate Professor of Business Law, TBS Business School (Toulouse, France). The author may be contacted at g.voss@tbs-education.fr.

Analytics tracking cookies. Finally, lessons for compliance are drawn, prior to concluding remarks.

CONTENTS

INTRODUCTION

Data are taking a more and more central role in the economy, whether they are personal data, sector-specific data, or other forms of data. However, due to a range of policy concerns, governmental regulations such as localization requirements and cross-border transfer conditions are arising.[1] At the same time, cross-border data flows make up an important part of international trade, which such regulations risk impeding.[2] One major player in international trade is the European Union,[3] which today consists of twenty-seven member states.[4] The European Union's General Data Protection Regulation (GDPR)[5] even underscores the importance of personal data flows to international trade, stating that "[f]lows of personal data to and from countries outside the [European] Union and international organisations are necessary for the expansion of international trade and international cooperation," but cautioning that this creates new challenges and concerns for data protection.[6]

Data protection, as the term is used in the European Union,[7] incorporates elements of both economic and social regulation, and protects what is considered

---

[1] Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows*, OECD TRADE POL'Y PAPERS NO. 220 (2019), at 11-12, http://dx.doi.org/10.1787/b2023a47-en [https://perma.cc/5SQ4-A38C].

[2] W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485, 487-89 (2020) [hereinafter *Cross-Border Data Flows*].

[3] *See, e.g.*, *EU Position in World Trade*, EUR. COMM'N (Feb. 9, 2019), https://ec.europa.eu/trade/policy/eu-position-in-world-trade/ [https://perma.cc/A44V-ETVX] ("the EU is the biggest player on the global trading scene").

[4] *Facts and Figures on the Structure of the European Union*, EUR. UNION, https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/structure_en [https://perma.cc/GL8G-D7QT].

[5] Commission Regulation 2016/679 of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1 (EU) (repealing Directive 95/46/EC (General Data Protection Regulation)) [hereinafter GDPR].

[6] *Id.* at recital 101.

[7] Bygrave highlights the broad nature of this term, which is not identical to privacy: "Europeans often stress that the two are not identical, reserving 'data protection' for a set of norms that serve a broader range of interests than simply privacy protection." LEE A BYGRAVE, DATA

there to be a fundamental right.[8] Once personal data processing fits under the law, obligations apply to the parties collecting and processing such data, and rights benefit those to whom the data relate.[9] The Charter of Fundamental Rights of the European Union (Charter), provides that personal data which are to be protected "must be processed fairly for specified purposes and on the basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[10] These and other rights and requirements are developed more fully in the GDPR. Furthermore, "Compliance … shall be subject to control by an independent authority."[11] Under the GDPR, this may involve administrative fines going up to the greater of €20 million or 4% of annual turnover in the case of violations of provisions regarding transfers of personal data by companies.[12]

Given these constraints, certain businesses, whether American or other non-European, or even European, may wonder how they can comply with the GDPR and export personal data back to their home offices or to service providers outside of Europe. What are the legal provisions applicable to them? What measures are available to help them export the data? What limits apply?

I. OVERVIEW

A. Aims and Structure of This Study

This study discusses compliance under the GDPR with respect to cross-border data transfer restrictions after the important *Schrems II* ruling of the Court of Justice of the European Union (CJEU) announced on July 16, 2020.[13] In doing so, it attempts to provide a holistic view of the legal parameters involved, developments past and future, and potential compliance action. It supplements this through relevant guidance and an analysis of enforcement cases. The hope is that the reader will leave not only with a fuller understanding of the challenges of GDPR compliance in cross-border data transfers, but also with a view of potential pathways to navigate those challenges.

PRIVACY LAW 26 (2014). Not only is EU data protection legislation "omnibus," covering both public and private processing of personal data, regardless of sector, it is based on data protection principles derived from earlier EU Member State law and the fair information practice principles (FIPPs), including data security requirements. *See* W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405, 420-22 (2019).

[8] ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 9 (2015).

[9] *Id*. at 14.

[10] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1 [hereinafter Charter], art. 8(2).

[11] *Id*. at art. 8(3).

[12] GDPR, *supra* note 5, at art. 83(5)(c).

[13] Case C-311/18 Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximilian Schrems, ECLI:EU:C:2020:559 (July 16, 2020) [hereinafter Schrems II].

The issue of cross-border data transfer requirements is crucial as compliance with such requirements is considered the most difficult task of privacy professionals, according to a recent report.[14] More particularly, this study focuses on transatlantic data flows between the European Union and the United States, given the significance of the trade relationship between those two blocs.[15] However, the discussion should be informative for personal data transfers to other areas of the world, as the *Schrems II* decision has implications for data transfers worldwide, which will be seen in this study's discussion of that case. However, the choice of the United States as the destination country in this study is significant. Not only are more and more nations adopting privacy laws, but the lack of a robust U.S. federal privacy law means that the U.S. companies may risk more and more regulatory "challenges" and distrust, not just in Europe, but worldwide.[16]

Following this Overview, this article describes cross-border data transfer restrictions under the GDPR and the *Schrems II* decision. Secondly, this article discusses ongoing negotiations between the European Union and the United States to reach an agreement on personal data transfers. Third, this article studies a new 2021 version of a data transfer tool—standard contractual clauses. Fourth, this article introduces and analyzes supplemental measures used to safeguard cross-border flows. In doing so, I consider 2020 and 2021 recommendations from the European Data Protection Board (EDPB), which is the EU institution created to ensure consistent application of the GDPR and to provide advice and guidelines about the GDPR (among its other tasks).[17] Fifth, this article draws lessons for compliance. Finally, this article ends with concluding remarks.

Now, for the remainder of this Overview this study sets out the context for transatlantic cross-border data flows under the GDPR and for the *Schrems II* decision. First, this study further introduces the GDPR, Europe's new data

---

[14] IAPP-EY ANNUAL PRIVACY GOVERNANCE REPORT 2021 2 (IAPP & EY eds., 2021), https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf [https://perma.cc/P6JG-9R7W] ("Complying with cross-border data transfer requirements" placed by far first among the responses, being selected by 59% of the privacy professionals surveyed, with the next highest response twenty points behind it, in response to the question: "Considering privacy and data protection laws around the world, which of the following tasks is most difficult to comply with?").

[15] *See, e.g.*, DANIEL S. HAMILTON & JOSEPH P. QUINLAN, THE TRANSATLANTIC ECONOMY 2021: ANNUAL SURVEY OF JOBS, TRADE AND INVESTMENT BETWEEN THE UNITED STATES AND EUROPE 17 (2021), https://www.uschamber.com/assets/archived/images/transatlanticeconomy2021_fullreport_lr.pdf [https://perma.cc/M4QD-6RM9] ("the largest commercial relationship in the world stretches across the Atlantic. Total transatlantic foreign affiliate sales were estimated at $6.2 trillion in 2019, easily ranking as the top commercial artery in the world on account of the thick investment ties between the two parties.").

[16] Justin Sherman, *Weak US Privacy Law Hurts America's Global Standing*, WIRED (July 20, 2021, 08:00 AM), https://www.wired.com/story/weak-us-privacy-law-hurts-americas-global-standing/ [https://perma.cc/Q693-UN53].

[17] GDPR, *supra* note 5, at art. 70(1).

protection legislation. Then, I briefly sketch the historical background of the Safe Harbor, *Schrems I*, and the establishment of the Privacy Shield.

B. Introduction to the GDPR

Since May 25, 2018,[18] the GDPR has applied with extraterritorial effect on many companies, individuals, and public bodies,[19] including those with no establishment in the European Union but who process[20] personal data[21] of individuals ("data subjects"[22]) located in the European Union related to: (i) the offering of goods or services to them, whether for pay or not,[23] or to (ii) the monitoring of data subject behavior to the extent it occurs in the European Union.[24] In applying (i) above, the EDPB has established a "targeting criterion" to determine whether an individual has been intentionally targeted for the offer of goods or services.[25] In certain cases covered by the territorial scope of Article 3 of the GDPR, a cross-border data transfer may occur.[26] The GDPR continues a cross-

---

[18] On May 25, 2018, the previous EU data protection legislation—Directive 95/46/EC—was repealed, and references to it were construed as references to the GDPR. *Id*. at art. 94. On that same date, the GDPR became applicable. *Id*. at art. 99(2).

[19] *See*, *e.g*., Manuel Klar, *Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies*, 11 HASTINGS SCI. & TECH. L.J. 101, 105-110 (2020).

[20] The term "processing" is broadly defined to include almost anything one can imagine doing with personal data. It refers to, "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, *supra* note 5, at art. 4(2).

[21] "Personal data" is intended broadly to include "any information relating to an identified or identifiable natural person." *Id*. at art. 4(1). Its scope is generally considered larger than that of the typical U.S. terms, "personal information" or "personally-identifiable information." *See* W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L.J. 287, 313-24 (2019) [hereinafter *Personal Data and the GDPR*].

[22] A "data subject" is an identified or identifiable individual, or natural person, to whom personal data relates. GDPR, *supra* note 5, at art. 4(1).

[23] *Id*. at art. 3(2)(a).

[24] *Id*. at art. 3(2)(b).

[25] EURO. DATA PROT. BOARD, *Guidelines 3/2018 on the Territorial Scope of the GDPR*, *Version 2.1 15*, (Nov. 12, 2019), [hereinafter *Guidelines 3/2018*] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [https://perma.cc/2XZ3-RUFA]. For a discussion of these Guidelines, *see* W. Gregory Voss, *Airline Commercial Use of EU Personal Data in the Context of the GDPR,* British Airways *and* Schrems II, 19 COLO. TECH. L.J. 377, 390-392 (2021) [hereinafter *Airline Commercial Use of EU Personal Data*].

[26] EURO. DATA PROT. BOARD, *Guidelines 05/2021 on the Interplay Between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR* 4 (Nov. 18, 2021) [hereinafter *Guidelines 05/2021*], https://edpb.europa.eu/system/files/2021-

border personal data transfer restriction found in prior legislation, which is addressed in Part II.A.

The GDPR succeeded and repealed Directive 95/46/EC (1995 Directive),[27] which first helped achieve a degree of EU data protection law harmonization following its adoption in 1995 and subsequent implementation in EU member state laws.[28] While the 1995 Directive had as one of its two stated objectives the prohibition of restrictions on the free flows of personal data between EU member states based on data protection grounds,[29] it also established a limitation on the export of personal data outside of the European Union, prohibiting it unless the destination country, known as a "third country," ensured an "adequate level of protection"[30] for such data, as discussed in Part I. However, the United States was not generally considered to have an adequate level of data protection,[31] and thus this cross-border data transfer limitation threatened to halt personal data exports from the European Union to the United States.[32]

C. The Safe Harbor, Schrems I, *and the Establishment of the Privacy Shield*

Given the important commercial relationship between the United States and the European Union,[33] the threatened halt to cross-border personal data flows between the two gave reason for fear for U.S. data importers.[34] Accordingly, in 2000, the European Commission ("Commission") and the U.S. Department of Commerce ("DoC") attempted to find a solution, and eventually negotiated a data governance framework, which was formalized in a Commission adequacy

---

11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf [https://perma.cc/RZ93-6J4E].

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 Oct., 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter 1995 Directive].

[28] *See, e.g.*, Priscilla M. Regan, *The Globalization of Privacy: Implications of Recent Changes in Europe*, 52 AM. J. ECON. & SOC. 257, 258 (1993) (Discussing that then proposed 1995 Directive would require the then twelve EU member states "to harmonize their privacy or data protection legislation," and noting variation in national laws "can be a barrier to the transfer of personal information from one country to another and a barrier to the operation of the global economic system.").

[29] 1995 Directive, *supra* note 27, at art. 1(2).

[30] *Id.* at art. 25(1).

[31] *See, e.g.*, CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 319 (2016) ("While adequate does not mean equivalent, it is clear that the United States in the 1990s lacked safeguards comparable to the directive.").

[32] Rändi Bessette & Virginia Haufler, *Against All Odds: Why There Is No International Information Regime*, 2 INT'L STUD. PERSP. 69, 80 (2001).

[33] *See, e.g.*, W. KUAN HON, DATA LOCALIZATION LAWS AND POLICY: THE EU DATA PROTECTION INTERNATIONAL TRANSFERS RESTRICTION THROUGH A CLOUD COMPUTING LENS 162 (2017) ("The Safe Harbour scheme was accordingly proposed as a Mechanism to facilitate US transfers, given the high volumes of EU-US trade.").

[34] HOOFNAGLE, *supra* note 31, at 319 ("American businesses and policy-makers were in a near panic in 1998, with implementation of the directive looming.").

decision known as the Safe Harbor Decision.[35] U.S. companies desirous of importing EU personal data to the United States could self-certify themselves as being compliant with the Safe Harbor privacy principles, issued by DoC and annexed to the Safe Harbor Decision,[36] and continue to import data to the United States.[37] These principles were intended to provide the data subjects of the data with rights and protections comparable to those under the 1995 Directive.[38] For most companies, the U.S. Federal Trade Commission ("FTC") held responsibility for monitoring this compliance, while the U.S. Department of Transportation ("DoT") had jurisdiction for airlines and travel agents.[39] Those companies excluded from FTC and DoT jurisdiction, essentially those in the telecommunications and financial sectors, were also excluded from the Safe Harbor agreement.[40]

However, while it had jurisdiction in most cases, the FTC took several years before it began to proactively monitor Safe Harbor compliance.[41] Shortly afterward, the Commission had reviewed and criticized the Safe Harbor agreement and provided recommendations for its reform in a 2013 report.[42] In the interim, U.S. intelligence contractor employee Edward Snowden had revealed U.S. mass surveillance programs and the role of U.S. technology giants ("U.S. Tech

---

[35] 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 Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7 [hereinafter Safe Harbor Decision].

[36] *Id*. at 10.

[37] *See* W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. INTERNET L. 1, 9 (May 2016) [hereinafter *The Future of Transatlantic Data Flows*].

[38] *See* CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 161 (2013) ("The EU-US Safe Harbor forms an intermediate plane between conflicting regulatory regimes which stops short of full harmonization, but which results in data importers in the US abiding by standards based on EU data protection law with regard to data imported from the EU" (citing Paul Schiff Berman, *Global Legal Pluralism*, 80 S. CAL. L. REV. 1155, 1227 (2007)); *see also The Future of Transatlantic Data Flows*, *supra* note 37, at 9.

[39] FTC jurisdiction was excluded for banks, savings and loans, credit unions, telecommunications and interstate transportation common carriers, air carriers, packers, and stockyard operators. Also, certain state-regulated insurance business is excluded from FTC jurisdiction. Furthermore, the U.S. Department of Transportation had jurisdiction with respect to airlines and travel agents. *See* Safe Harbor Decision, *supra* note 35, at Annex VII.

[40] *See, e.g*., ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 39 (2008) ("Because the Federal Trade Commission jurisdiction does not extend to financial services or telecommunications, these sectors are excluded from the agreement.").

[41] *See* Chris Connolly & Peter van Dijk, *Enforcement and Reform of the EU-US Safe Harbor Agreement*, *in* ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES 261, 277-81 (David Wright & Paul De Hert, eds., 2016); *see also The Future of Transatlantic Data Flows*, *supra* note 37, at 11.

[42] *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM (2013) 847 final (Nov. 27, 2013).

Giants") in cooperating with the authorities in these programs.[43] At the same time, it was revealed that U.S. intelligence had hacked telephone communications of Europeans such as German leader Angela Merkel.[44] These revelations had a significant impact on European views of the U.S. Tech Giants and of the U.S. intelligence activities[45] and helped partisans of the GDPR overcome the effect of massive lobbying and eventually adopt a version of that legislation on first reading in the European Parliament sitting in plenary.[46]

These same revelations of U.S. mass surveillance were at the heart of the *Schrems I* decision, in which the CJEU invalidated the Safe Harbor Decision on October 6, 2015.[47] In the case, Maximilian Schrems argued that personal data

---

[43] *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/CB83-V87D]; *see also* Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), https://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?smid=url-share [https://perma.cc/BK6A-JZM9] (identifying Edward Snowden as the source of the revelations).

[44] *See, e.g.*, Ian Traynor, Philip Oltermann & Paul Lewis, *Angela Merkel's Call to Obama: Are You Bugging My Mobile Phone?*, GUARDIAN (Oct. 24, 2013), https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german [https://perma.cc/F46D-TY7Z].

[45] *See, e.g.*, Simon Davies, *Privacy Opportunities and Challenges with Europe's New Data Protection Regime*, *in* PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS 55, 57 (Marc Rotenberg, Julia Horwitz & Jeramie Scott, eds., 2015) ("The negative perspective of U.S. attitudes toward the privacy protection of Europeans is not confined to security operations. Indeed there's a widespread view among policy makers that none of the U.S. administrations from Clinton onward have delivered on commitments to reform the arenas of privacy and surveillance at the international level.").

[46] *See* Nikhil Kalyanpur & Abraham L. Newman, *The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation*, 57 J. COMMON MKT. STUD. 448, 462 (2019) ("While business groups dominated early discussions, a former Senior Department of Commerce official summarized, '. . . along comes Mr. Snowden and everything goes into a tailspin.' He noted that 'the Parliament was having a very difficult time coming to an agreement on the legislation and then the logjam broke.'"); *see also* Nikhil Kalyanpur & Abraham Newman, *Today, a New E.U. Law Transforms Privacy Rights for Everyone. Without Edward Snowden, It Might Never Have Happened.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/ [https://perma.cc/YS7S-GX4L] ("The leaks catapulted the GDPR into the public spotlight….Pro-consumer members of the European Parliament, like Jan Albrecht, capitalized on public attention by condemning the influence of foreign firms in the lobbying process."); W. Gregory Voss, *Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later*, 17(9) J. INTERNET L. 1, 19 (2014) ("Even the lobbyists have recognized the effect of the NSA PRISM disclosures on the advance of EU data protection legislative reform, however.").

[47] Case C-362/14 Maximilian Schrems v. Data Prot. Comm'r, 2015 E.C.R. 000 [hereinafter Schrems I].

from his Facebook account, which was collected and processed under the responsibility of Facebook Ireland Ltd (the controller[48]), would be transferred to parent Facebook Inc. (now Meta) in the United States, where it would be subject to potential access by the authorities, without the same safeguards as in the European Union.[49] Following that decision, in 2016, EU and U.S. authorities negotiated a replacement personal data transfer framework—the EU-U.S. Privacy Shield, which then benefitted from an adequacy decision of the Commission (Privacy Shield Decision).[50] These data agreements were safeguards then available in order to transfer personal data to the United States, and thus to avoid a blocking of data flows by the cross-border personal data transfer restrictions under EU data protection law, the current version of which—the GDPR—is discussed in Part II.A.

II. RESTRICTIONS OF CROSS-BORDER PERSONAL DATA TRANSFERS UNDER THE GDPR AND *SCHREMS II*

This Part begins by setting out the legislative provisions of the GDPR restricting certain cross-border transfers of personal data. Subsequently, the *Schrems II* decision and its context are examined in detail.

A. GDPR Cross-Border Transfer Restriction

The GDPR provides for a restriction of cross-border personal data transfers, limiting them to third countries that provide an adequate level of data protection, with the relevant provisions applied "to ensure that the level of protection of natural persons guaranteed by [the GDPR] is not undermined."[51] The term "third country" must now be read as a country outside of the European Economic Area (EEA), which includes the now twenty-seven EU member states, and three member states of the European Free Trade Association (Iceland, Liechtenstein, and Norway).[52] In order to become applicable throughout the EEA the GDPR needed to be incorporated into the EEA Agreement by an EEA Joint Committee Decision.[53] Such a decision was issued on July 6, 2018, and so the GDPR was

---

[48] *See* GDPR, *supra* note 5, at art. 4(7) (A controller is defined as "the natural or legal personal, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data").

[49] *See The Future of Transatlantic Data Flows*, *supra* note 37, at 10.

[50] 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 O.J. (L 207/1) [hereinafter Privacy Shield Decision].

[51] GDPR, *supra* note 5, at art. 44.

[52] *Glossary: Third country*, THOMSON REUTERS PRACTICAL LAW, https://uk.practicallaw.thomsonreuters.com/w-014-8210?contextData=%28sc.Default%29&transitionType=Default [https://perma.cc/4MTP-DCZE?type=image].

[53] *See Incorporation of the GDPR into the EEA Agreement*, EFTA (Apr. 13, 2018), https://www.efta.int/EEA/news/Incorporation-GDPR-EEA-Agreement-508041 [https://perma.cc/G9BQ-ACFW].

incorporated into the EEA Agreement,[54] with effect from July 20, 2018.[55] The GDPR provides that "The free movement of personal data within the [European] Union shall neither be restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[56] However, today this provision should be read to extend to all of the EEA.

There is no definition in the GDPR of the notion of a personal data transfer to a third country or an international organization. However, the EDPB has recently identified three criteria which when cumulated indicate that there is such a transfer:

(1) A controller or a processor[57] is subject to the GDPR for the given processing.

(2) This controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer").

(3) The importer is in a third country or is an international organisation, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.[58]

It should be kept in mind that for point 1 above to apply, the territorial scope requirements of Article 3 of the GDPR must be met, such that the controller or processor falls within the ambit of the legislation.[59] Furthermore, the EDPB advises that no transfer is considered to have occurred when a data subject discloses his or her data directly and on his or her initiative to the recipient,[60] nor does one exist where there is no different controller or processor receiving or

---

[54] *See* Decision of the EEA Joint Committee No. 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022], 2018 O.J. (L 183) 23 (The national legislation of the three EEA-EFTA countries had to be amended pursuant to the GDPR in order for the EEA act to take effect.); *General Data Protection Regulation incorporated into the EEA Agreement*, EFTA (July 6, 2018), https://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291 [https://perma.cc/3BPH-QLPL].

[55] *General Data Protection Regulation (GDPR) entered into force in the EEA*, EFTA (July 19, 2018), https://www.efta.int/EEA/news/General-Data-Protection-Regulation-GDPR-entered-force-EEA-509576 [https://perma.cc/G8S8-N8EY] ("The GDPR is now applicable throughout the Internal Market, including the EEA EFTA States Iceland, Liechtenstein and Norway.").

[56] GDPR, *supra* note 5, at art. 1(3).

[57] *Id.* at art. 4(8) (A processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."); *see supra* note 48 (for a definition of "controller").

[58] *Guidelines 05/2021*, *supra* note 26, at 4.

[59] *Guidelines 3/2018*, *supra* note 25, at 5.

[60] *Guidelines 05/2021*, *supra* note 26, at 5.

being given access to the data.[61] In those cases, the requirements of point 2 above are not satisfied. However, intra-group data disclosures may be considered transfers, depending on the circumstances.[62] The EDPB underscores the point that:

> … controllers and processors whose processing is subject to the GDPR pursuant to Article 3 always have to comply with Chapter V of the GDPR when they disclose personal data to a controller or processor in a third country or to an international organisation. This also applies to disclosures of personal data carried out by controllers/processors which are not established in the EU but are subject to the GDPR pursuant to Article 3(2) to a controller or processor in the same or another third country.[63]

When a cross-border transfer has occurred, the overall legal framework of the European Union no longer applies, so other forms of protection for personal data must be provided, such as the transfer being made in connection with a Commission adequacy decision or providing appropriate safeguards for data protection.[64] A cross-border transfer outside of the EEA may take place if the destination country or international organization benefits from a Commission adequacy decision. This means that when "the Commission has decided that the third country, a territory or one or more specified sectors within the third country, or the international organisation in question ensures an adequate level of protection," a transfer may occur without specific authorization.[65] Such was the case with respect to companies on the Privacy Shield Decision (Privacy Shield Decision)[66] List, until the *Schrems II* decision. While the list of countries benefitting from a Commission adequacy was recently lengthened by the addition of the Republic of Korea on December 17, 2021,[67] it is still rather short. In addition to South Korea, adequacy has now been recognized for Andorra, Argentina, Canada (for commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom under both the

---

[61] *Id*. at 6 (for there to be a transfer "there must be a controller or processor disclosing the data (the exporter) and a different controller or processor receiving or being given access to the data (the importer).").

[62] *Id*. at 7 (there would be a transfer if, say, the exporter and importer are "separate controllers or processors").

[63] *Id*. at 9.

[64] *Id*. at 3.

[65] GDPR, *supra* note 5, at art. 45(1).

[66] Privacy Shield Decision, *supra* note 50, at art. 1(1) ("For the purposes of Article 25(2) of Directive 95/46/EC, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield."). *See id*. at art. 1(3) ("For the purpose of paragraph 1, personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included on the 'Privacy Shield List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II.").

[67] Commission Implementing Decision of 17.12.2021, C(2021) 9316 final (Dec. 17, 2021).

GDPR and the Law Enforcement Directive (LED) (Directive (EU) 2016/680), and Uruguay.[68]

Otherwise, appropriate safeguards such as standard contractual clauses (SCCs),[69] or binding corporate rules (BCRs)[70] may be used as a basis for transfer under certain conditions. Binding corporate rules (or BCRs) are defined as:

> personal data protection policies which are adhered to by a controller or processed established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in joint economic activity.71

Thus, unlike SCCs, BCRs are reserved to transfers within corporate and other undertaking groups.

However, in a recent trade association study, eighty-five per cent of companies surveyed were estimated to use SCCs, making them by far the most widely used data transfer mechanism.[72] Only five percent of companies surveyed were using other data transfer mechanisms.[73] Moreover, SCCs were clearly the target for invalidation in the *Schrems II* litigation.

B. Schrems II *Proceedings and Ruling*

During the investigation by the Irish supervisory authority[74] (Data Protection Commission (DPC)) of the facts related to the *Schrems I* case, Facebook revealed that a "large part" of the personal data it transferred was done so using SCCs.[75] At the suggestion of the DPC Commissioner, Maximilian Schrems made a reformulated complaint asking the Irish Data Protection Commissioner to suspend or prohibit the transfer of his data by Facebook Ireland to the U.S. parent company Facebook Inc., based on his assertion that U.S. law requires Facebook to make the data it transfers available to the U.S. authorities, such as the NSA, and that the such data are used in ways incompatible with the rights to privacy and data protection, and the right to an effective remedy and to a fair

---

[68] *Adequacy Decisions*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/3KPS-F8LN].

[69] *See* Part IV *infra*.

[70] GDPR, *supra* note 5, at art. 47.

[71] *Id*. at art. 4(20).

[72] SCHREMS II IMPACT SURVEY REPORT 5 (2020), https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf [https://perma.cc/Q4EW-7V2G].

[73] *Id*. at 8.

[74] GDPR, *supra* note 5, at art. 4(21). A "supervisory authority" is "an independent public authority which is established by a Member State pursuant to Article 51" of the GDPR. Supervisory authorities are commonly referred to as data protection authorities (DPAs), or data regulators.

[75] Schrems II, *supra* note 13, at para. 54.

trial[76] under the Charter of Fundamental Rights of the European Union ("Charter"). The DPC Commissioner brought an action before the High Court in Ireland, so that it could be referred to the CJEU on the validity of the 2010 SCC adequacy decision ("SCC Decision") of the Commission, which was at issue in Schrem's reformulated complaint. The Irish High Court—the referring court—had established findings that the U.S. authorities' intelligence activities related to personal data transferred to the United States were based on Section 702 of the FISA (U.S. Foreign Intelligence Surveillance Act) and on E.O. 12333, and that non-U.S. persons are covered only by PPD-28, as to limitations on intelligence activities, and that only specifies that intelligence activities should be "as tailored as feasible." In its request for reference preliminary ruling, the referring court "asks whether the SCC Decision may be considered to be valid," despite the SCCs not being binding on the U.S. authorities.

In *Schrems II*, the CJEU found that there was nothing in the SCC Decision that prevented supervisory authorities from "suspending or prohibiting, as appropriate, a transfer of personal data to a third country" made using the SCCs annexed to that decision, under the Charter of Fundamental Rights of the European Union ("Charter").[77] The DPC Commissioner brought an action before the High Court in Ireland, so that it could be referred to the CJEU on the validity of the 2010 SCC adequacy decision ("SCC Decision")[78] of the Commission, which was at issue in Schrem's reformulated complaint.[79] The Irish High Court—the referring court—had established findings that the U.S. authorities' intelligence activities related to personal data transferred to the United States were based on Section 702 of the FISA (U.S. Foreign Intelligence Surveillance Act) and on E.O. 12333,[80] and that non-U.S. persons are covered only by PPD-28, as to limitations on intelligence activities, and that only specifies that intelligence

---

[76] *Id*. at para. 55.

[77] Charter, *supra* note 10, at arts. 7, 8, & 47 (the relevant articles of the Charter are arts. 7 (Respect for private and family life (Privacy)), 8 (Protection of personal data), and 47 (Right to an effective remedy and to a fair trial)).

[78] Commission Decision of 5 Feb., 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU, 2010 O.J. (L 39) 5 [hereinafter SCC Decision].

[79] Schrems II, *supra* note 13, at para. 57. For a discussion of the various versions of the SCC decisions, *see* Part IV *infra*.

[80] Schrems II, *supra* note 13, at para. 60. "FISA Section 702" refers to Section 702 of the FISA Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. § 1881a). For a discussion of FISA Section 702, *see generally* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015). For a short overview, *see* EDWARD C. LIU, CONG. RESEARCH SERV., IF11451, FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA): AN OVERVIEW (2021). E.O. 12333 refers to U.S. Executive Order 12,333, Exec. Order No. 12,333, 46 Fed. Reg. 59, 941 (1981). For a short discussion of E.O. 12333, *see* Chris D. Linebaugh & Edward C. Liu, CONG. RESEARCH SERV., R46724, EU DATA TRANSFER REQUIREMENTS AND U.S. INTELLIGENCE LAWS: UNDERSTANDING SCHREMS II AND ITS IMPACT ON THE EU-U.S. PRIVACY SHIELD 10-11 (2021).

activities should be "as tailored as feasible."[81] In its request for reference preliminary ruling, the referring court "asks whether the SCC Decision may be considered to be valid," despite the SCCs not being binding on the U.S. authorities.[82]

The DPC Commissioner had not made a final decision on Schrems' complaint prior to the date of application of the GDPR,[83] thus the questions referred to the CJEU were decided with reference to the GDPR which by then had repealed and replaced the 1995 Directive.[84] The CJEU in *Schrems II* highlighted the fact that Article 46(1) of the GDPR "states that data subjects must be afforded appropriate safeguards, enforceable rights and effective legal remedies."[85] The standard applied by the CJEU, was whether the level of protection provided by SCCs to the data subject's personal data was "essentially equivalent to that guaranteed within the European Union" by the GDPR.[86] This standard of "essentially equivalent" was already invoked by the CJEU in its *Schrems I* decision, in which it was stated with respect to a Commission adequacy decision that:

> [I]n order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order[.][87]

The predecessor to the EDPB under the 1995 Directive—the Article 29 Data Protection Working Party—advised that "the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation."[88]

In *Schrems II*, the CJEU found that there was nothing in the SCC Decision that prevented supervisory authorities from "suspending or prohibiting, as appropriate, a transfer of personal data to a third country" made using the SCCs annexed to that decision,[89] and that "effective mechanisms which, in practice, ensure that the transfer to a third country of personal data" pursuant to the SCCs, "is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them" are provided by the SCC

---

[81] Schrems II, *supra* note 13, at para. 64.

[82] *Id*. at para. 67.

[83] *Id*. at para. 77.

[84] *Id*. at para. 79 ("The questions referred for a preliminary ruling must therefore be answered in the light of the provisions of the GDPR rather than those of Directive 95/46").

[85] *Id*. at para. 103.

[86] *Id*. at para. 105.

[87] Schrems I, *supra* note 47, at para. 96.

[88] ARTICLE 29 DATA PROT. WORKING PARTY, *Adequacy Referential*, WP 254 REV.01 (Feb. 6, 2018), available at https://ec.europa.eu/newsroom/article29/items/614108 [https://perma.cc/R9UL-HLMB]. The EDPB endorsed this referential. *See* EURO. DATA PROT. BOARD, *Endorsement 1/2018* at 2 (May 25, 2018), available at https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf [https://perma.cc/22DD-F547].

[89] Schrems II, *supra* note 13, at para. 146.

Decision.[90] Accordingly, the validity of the SCC Decision was not affected,[91] although certain conditions had to be met for their use. Indeed, SCCs cannot bind public authorities[92] and so, depending on the circumstances, controllers may need to adopt supplementary measures to ensure compliance with the required level of data protection[93]:

> It is therefore, above all, for that 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, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.[94]

Thus, following a case-by-case analysis, the exporter of personal data may need to adopt measures to supplement the SCCs.

However, the CJEU also examined the validity of the Privacy Shield Decision, which "enables interference, based on national security and public interest requests or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States," which could result from "access to, and use of, personal data transferred from the European Union to the United States by US public authorities through the PRISM and UPSTREAM surveillance programmes under Section 702 of the FISA and E.O. 12333."[95] The fundamental rights concerned, the right to privacy and the right to data protection (Articles 7 and 8 of the Charter) are not absolute, and "must be considered in relation to their function in society,"[96] however any limitation to them may be made only if it is "necessary and genuinely meets objectives of general interest recognised by the [European] Union or the need to protect the rights and freedoms of others."[97] The CJEU found that under Section 702 of the FISA there were no limitations "on the power it confers to implement surveillance programmes for the purpose of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes."[98] Furthermore, PPD-28 did not "grant data subjects actionable rights before the courts against the US authorities," and so the Privacy Shield Decision could not ensure an essentially equal level of protection to that of the Charter, due to a lack of effective and enforceable rights for data subjects.[99] A similar situation exists with respect to E.O.

---

[90] *Id*. at para. 148.
[91] *Id*. at para. 149.
[92] *Id*. at para. 132.
[93] *Id*. at para. 133.
[94] *Id*. at para. 134.
[95] *Id*. at para. 165.
[96] *Id*. at para. 172.
[97] *Id*. at para. 174.
[98] *Id*. at para. 180.
[99] *Id*. at para. 181.

12333.[100] Yet, the Commission was supposed to take account of "effective administration and judicial redress for the data subjects whose personal data are being transferred," when assessing adequacy.[101]

After reviewing the Privacy Shield Decision Ombudsperson mechanism, which was held up as a redress mechanism, the CJEU found that there was nothing in the Privacy Shield Decision to indicate that the decisions of the Ombudsperson would bind the intelligence services, nor that political claims about the independence of the Ombudsperson were backed up by legal safeguards on which data subjects could rely.[102] Accordingly, the CJEU found that the Privacy Shield Decision "does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter."[103] As a result, Article 1 of the Privacy Shield Decision was incompatible with the requirements for an adequacy decision under the GDPR,[104] and Article 1's invalidity affected the validity of the adequacy decision in its entirety,[105] and therefore "… it is to be concluded that the Privacy Shield Decision is invalid."[106]

Thus, the Privacy Shield Decision has been invalidated and is no longer a mechanism available for transfers of EU personal data to the United States, however, as discussed above, SCCs—the new version of which is detailed in Part IV—were not invalidated, and might still be used under certain conditions as considered in Parts V, VI and VII, and the CJEU mentioned that derogations might also be available under Article 49 of the GDPR.[107] Yet, these derogations are "to be interpreted restrictively and used sparingly," to quote one commentator,[108] and their focus on specific situations limits their value in large data processing schemes. As a result, this study will focus on the use of SCCs. However, before developing its analysis of SCCs further, this study now turns to the possibility of a replacement for the Privacy Shield Decision.

III. A PRIVACY SHIELD REPLACEMENT?

Following *Schrems II*, the question that was immediately asked was, will there be a Privacy Shield replacement? This Part considers that question, first by examining the negotiations to-date. Then, the new EU-US Trade and Technology Council is introduced. U.S. Big Tech input and possible paths forward to unblock the situation are discussed, as is the recently announced Trans-Atlantic Data Privacy Framework, prior to setting out the procedure for adopting a new

---

[100] *Id*. at para. 182.

[101] GDPR, *supra* note 5, at art. 45(2)(a).

[102] Schrems II, *supra* note 13, at para. 196.

[103] *Id*. at para. 197.

[104] *Id*. at para. 199.

[105] *Id*. at para. 200.

[106] *Id*. at para. 201.

[107] *Id*. at para. 202.

[108] CHRISTOPHER KUNER, LEE A. BYGRAVE & CHRISTOPHER DOCKSEY, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 841, 846 (2020).

adequacy decision on any eventual Privacy Shield replacement. Finally, a conclusion is drawn with respect to this Part.

A. Negotiation on a Replacement for the Privacy Shield

Shortly after the CJEU rendered its *Schrems II* judgment, the U.S. Secretary of State said that the United States would "continue to work closely with the EU to find a mechanism to enable the essential unimpeded commercial transfer of data from the EU to the United States."[109] That autumn, the United States, the European Union and the United Kingdom (which was then still applying the GDPR) were all reported to be trying to establish separate agreements on data transfers—between the European Union and the United States, between the European Union and the United Kingdom, and between the United States and the United Kingdom, in the hopes of having such agreements by early 2021 at the latest.[110] Presently, two out of three of the proposed agreements have either been reached or significantly advanced: in June 2021 the Commission issued its adequacy decision for UK data protection under the United Kingdom General Data Protection Regulation (UK GDPR),[111] and in December 2021 the United States and the United Kingdom announced that they had made "significant progress … to support, stabilize and realize the benefits of bilateral data flows," and they were committed to an enduring UK-U.S. data partnership.[112] However, the recently announced political agreement in principle for a replacement to the Privacy Shield has yet to be finalized.

B. EU–US Trade and Technology Council (TTC)

On March 25, 2021, the U.S. Commerce Secretary and the EU Justice Commissioner indicate the intent to intensify negotiations on a replacement to the Privacy Shield.[113] Just before the summer, the two governments recalled that they have "the largest economic relationship in the world," established a high-level EU-US Trade and Technology Council (TTC), and committed "to work together to ensure safe, secure, and trusted cross-border data flows that protect

---

[109] Michael R. Pompeo, *European Court of Justice Invalidates EU-U.S. Privacy Shield*, U.S. DEP'T. OF STATE (July 17, 2020), https://2017-2021.state.gov/european-court-of-justice-invalidates-eu-u-s-privacy-shield/index.html. [https://perma.cc/C4A2-TXKB].

[110] Mark Scott & Vincent Manancourt, *What You Need to Know About EU, US and UK Data Talks*, POLITICO (Nov. 2, 2020, 6:30 AM), https://www.politico.eu/article/uk-eu-us-privacy-data-protection-negotiations/. [https://perma.cc/8WA6-EYZ7].

[111] Commission Implementing decision of 28 June, 2021 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom, C(2021) 4800 (June 28, 2021).

[112] *U.S. – U.K. Joint Statement on Deeping the Data Partnership*, U.S. DEP'T. OF COM. (Dec. 8, 2021), https://www.commerce.gov/news/press-releases/2021/12/us-uk-joint-statement-deepening-data-partnership [https://perma.cc/SBF4-5RA9].

[113] Andrea Vittorio, *EU-U.S. Data Privacy Talks Pick Up as Companies Sit in 'Limbo'*, B L (Mar. 25, 2021 11:52 PM), https://news.bloomberglaw.com/privacy-and-data-security/eu-u-s-data-privacy-talks-pick-up-as-companies-sit-in-limbo [https://perma.cc/6GF5-6H5T].

consumers and enhance privacy protections, while enabling Transatlantic commerce."[114] The TTC has largely been seen as an effort to counter China's rise in technology sectors.[115] A little less than three months later, Commerce Secretary Raimondo stated that she was confident that "we will reach a durable resolution on an enhanced Privacy Shield framework that benefits us all."[116] However, this effort, which failed in June 2021 EU-U.S. summit,[117] did not yield a successful data transfer agreement at the inaugural meeting of the TTC on September 29, 2021.[118] Data flows were "off the table" from the TTC meeting, as the EU did not want these discussions mixed in with the TTC discussions.[119] Moreover, Commission officials have cautioned that the negotiation process could move slowly, and its Commissioner for Justice has said that it may be necessary for

[114] *EU-US Summit 2021 – Statement: Towards a renewed Transatlantic partnership*, WHITE HOUSE (June 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/ [https://perma.cc/K24H-BVBW] (in this context the two governments indicated their intention "to continue to work together to strengthen legal certainty in Transatlantic flows of personal data.").

[115] *See, e.g.*, Barbara Moens & Mark Scott, *Transatlantic Trade Deal Rises from the Grave to Fight China*, POLITICO (Sept. 9, 2021, 6:40 PM), https://www.politico.eu/article/ttip-rises-from-the-grave-to-fight-china/ [https://perma.cc/3J5V-6QA6] ("The first meeting of the Trade and Tech Council (TTC) in Pittsburgh on September 29 is intended to build a diplomatic platform for the European Union and the United States to work together on industrial and tech standards to counter China's rise in sectors ranging from microchips and robots to artificial intelligence and the alleged antirust abuses of Google and Amazon.") [hereinafter *Transatlantic Trade Deal*].

[116] Gina M. Raimondo, *Keynote Remarks by U.S. Secretary of Commerce Gina Raimondo at the Tallinn Digital Summit*, U.S. DEP'T OF COM. (Sept. 7, 2021), https://www.commerce.gov/news/speeches/2021/09/keynote-remarks-us-secretary-commerce-gina-raimondo-tallinn-digital-summit [https://perma.cc/M77L-VHF4].

[117] *Transatlantic Trade Deal*, *supra* note 115 ("As far as tech policy goes, Washington is trying to piggyback a renewed transatlantic data transfer deal onto TTC, after a failed attempt to do so at the EU-U.S. summit in June.").

[118] There is no mention of a data agreement in the statement issued following the TTC's first meeting. *See U.S.-EU Trade and Technology Council Inaugural Joint Statement*, WHITE HOUSE (Sept. 29, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/ [https://perma.cc/S8F7-LKW7].

[119] Vincent Manancourt & Mark Scott, *Washington Says a Transatlantic Data Deal Is Close. Brussels Disagrees.*, POLITICO (Sept. 17, 2021, 6:30 AM), https://www.politico.eu/article/washington-transatlantic-data-deal-brussels/ [https://perma.cc/3HLR-QC93] (reporting that at a meeting on September 15, 2021, between Commission officials and business and non-profit groups, "'They told us the EU doesn't want to include the privacy shield and data flows within the TTC umbrella,' said one of the participants. Margrethe Vestager, the EU's digital chief, also told POLITICO that discussions around data flows were off the table later this month.").

the United States to change its surveillance laws in order to allow for a new agreement.[120]

C. Input from U.S. Big Tech and Possible Paths to Unblock the Situation

Nonetheless, U.S. Big Tech has actively lobbied for the adoption of a replacement for the Privacy Shield. For example, on November 26, 2021, representatives of Facebook (Meta) met with Didier Reynders' staff prior to a meeting with the EU Justice Commissioner and indicated that Meta would like to discuss on a successor to the Privacy Shield and a timeline for a new agreement.[121] On December 1, 2021, representatives of Google met with Commissioner Reynders on, inter alia, international data flows. Reynders said that much progress had been made in EU-U.S. negotiations on the issue, but that "certain outstanding issues still remain," while on its side "Google expressed the hope that a solution can be found that would not require Congressional action."[122] Thus, Google seeks a replacement Privacy Shield agreement, without modifications to U.S. surveillance legislation, even though, paradoxically, it works with Big Tech colleagues at Amazon, Apple, Dropbox, Evernote, Google, Facebook (Meta), Microsoft, Snap, Inc., Twitter, Yahoo and Zoom in a Reform Government Surveillance (RGS) coalition that "strongly believes that current surveillance laws and practices must be reformed," and be made "consistent with established global norms of privacy, free expression, security, and the rule of law."[123]

Various commentators have opined that surveillance law reform is difficult[124] or unlikely,[125] although it seemed to be the key to unblocking the situation. An

---

[120] Catherine Stupp, *Officials Warn Privacy Shield Replacement May Be a Long Way Off*, WALL ST. J. (Sept. 8, 2020, 5:30 AM), https://www.wsj.com/articles/officials-warn-privacy-shield-replacement-may-be-a-long-way-off-11599557400 [https://perma.cc/6YVN-BSB3] ("Forging a new data-sharing agreement between the U.S. and European Union may require changes to surveillance laws, officials warned last week").

[121] Lucrezia Busa, *Minutes of the meeting with Meta and Cab Reynders 26/10/2021*, ASK THE EU, [https://perma.cc/S7VG-7ZFD] (The Reynders Cabinet member (Tuts) stressed "that the only way to provide legal certainty is to develop a solution that addresses all requirements of the Schrems II judgment, which may take some time.").

[122] Lucrezia Busa, *Minutes of the meeting with Google 01/12/2021*, ASK THE EU, [https://perma.cc/E38H-88TE].

[123] *Purpose and Members*, REFORM GOVERNMENT SURVEILLANCE, https://www.reformgovernmentsurveillance.com/about/ [https://perma.cc/H98F-9YRD].

[124] *See, e.g.*, Laurie Clarke, *After a Year of Limbo a EU-US Data Privacy Agreement Still Hangs in the Balance*, TECH MONITOR (Sept. 17, 2021), https://techmonitor.ai/policy/privacy-and-data-protection/eu-us-data-agreement-schrems-ii [https://perma.cc/62BJ-9JL7] (citing Georgetown Law professor Anupam Chander).

[125] *See, e.g.*, Matt Burgess, *Europe's Move Against Google Analytics Is Just the Beginning*, WIRED (Jan. 19, 2022, 05:07 PM), https://www.wired.com/story/google-analytics-europe-austria-privacy-shield/ [https://perma.cc/HU2C-VVCZ] (citing Gabriela Zanfir-Fortuna of the Future of Privacy Forum, a non-profit whose corporate supporters include [among many others] two Big Tech companies mentioned in this study: Google and Facebook). *See*

alternative proposal involves the use of executive orders to circumvent Congress.[126] Yet, executive orders are inherently unstable, and may be revoked, modified, or superseded by the same President or his or her successor.[127] This aspect will need to be taken into consideration by negotiators, and could potentially lead to a lack of security for companies relying on the Privacy Shield replacement, if the revocation of an executive order leads to an invalidation of that replacement instrument.

One possible path that has been put forward to unblock the negotiations is potentially providing greater oversight of U.S. security agencies, such as having judges decide on whether collection of EU personal data is legal.[128] However, we must remember that geopolitics has a role to play in the situation.[129]

Supporters, FUTURE OF PRIV. F., https://fpf.org/about/supporters/ [https://perma.cc/393K-DNMF].

[126] *See* Burgess, *supra* note 125.

[127] VIVIAN S. CHU & TODD GARVEY, CONG. RESEARCH SERV., RS20846, EXECUTIVE ORDERS: ISSUANCE, MODIFICATION, AND REVOCATION (Apr. 16, 2014), at 7.

[128] *See* Burgess, *supra* note 125. These judges should be independent, be able to rule on "whether U.S. collection of European data was lawful and proportionate," and potentially could be operated under the U.S. Office of the Director of National Intelligence. *See* Mark Scott, *US Offers Deal to Woo Europe on Data*, POLITICO (Oct. 21, 2021, 4:02 PM), https://www.politico.eu/article/negotiations-for-new-transatlantic-data-deal-nudge-forward/ [https://perma.cc/RBU8-94EQ].

[129] *The Future of EU-US Data Transfers*, PAOLO BALBONI (Sept. 24, 2021), https://www.paolobalboni.eu/index.php/2021/09/24/the-future-of-eu-us-data-transfers/ [https://perma.cc/UVA6-CBQE] ("This current situation perfectly demonstrates something which is not new, but that should not be ignored any longer: data protection is not only a legal matter, but also a geopolitical one. It's safe to say that we will be stuck in limbo for a little longer than some of us may have wished.").

D. Geopolitics and the Announcement of a New Trans-Atlantic Data Privacy Framework

Against the backdrop of the launch of Russia's "special military operation"[130] in the Ukraine, and subsequent close cooperation between the United States and the European Union to deal with this new geopolitical situation, the Western blocs reached an "agreement in principle" for a new cross-border data transfer framework.[131] The White House and the European Commission announced the agreement in principle on a new Trans-Atlantic Data Privacy Framework on March 25, 2022.[132] The United States is to implement "new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities."[133] However, the "legal documents" necessary to achieve this have yet to be drafted and agreed, although it was announced that U.S. commitments would come in an Executive Order.[134]

Truly, this agreement remains on the "in principle" level, as emphasized by the EU Justice Commissioner Didier Reynders, and details must still be worked

---

[130] This is the term used by Russian President Vladimir Putin to describe Russia's military offensive against the Ukraine. *See*, *e.g.*, United Nations, Security Council, Russian Federation Announces 'Special Military Operation' in Ukraine as Security Council Meets in Eleventh-Hour Effort to Avoid Full-Scale Conflict, SC/14803, Feb. 23, 2022, https://www.un.org/press/en/2022/sc14803.doc.htm [https://perma.cc/FJ4R-U2N6].

[131] *See* Vincent Manancourt & Mark Scott, *Political Pressure Wins Out as US Secures Preliminary EU Data Deal*, POLITICO (Mar. 25, 2022, 2:19 PM), https://www.politico.eu/article/privacy-shield-data-deal-joe-biden-ursula-von-der-leyen/ [https://perma.cc/7TWK-RX75] ("But in the weeks and days building up to the announcement, U.S. and European negotiators—who have spent almost two years hammering out details to give EU citizens greater control over their data when it's transferred to the U.S., while also allowing American national security agencies access to some of that information—had warned that final sticking points are yet to be hashed out." "Yet amid efforts to show renewed transatlantic unity following Russia's invasion of Ukraine, both von der Leyen and Biden cast those doubts aside."). *See also* Tanguy Van Overstraeten, Guillaume Couneson & Peter Church, *EU & US: The Trans-Atlantic Data Privacy Framework: A New Realpolitik for Data?*, LINKLATERS (Mar. 29, 2022), https://www.linklaters.com/en/insights/blogs/digilinks/2022/march/eu-and-us—-the-trans-atlantic-data-privacy-framework—-a-new-realpolitik-for-data [https://perma.cc/TC88-AUHA] ("More generally, the events in Ukraine may have provided an opportunity to re-assess the benefits of a strong transatlantic relationship, with the White House press release noting that the deal *reflects the strength of the enduring US-EU relationship, as we continue to deepen our partnership based on our shared democratic values*.") (internal quotations omitted).

[132] *United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework*, THE WHITE HOUSE (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/ [https://perma.cc/9YMR-TTYP].

[133] *Id.*

[134] *Id.*

out.[135] However, at a press conference on March 30, 2022, Commissioner Reynders called the agreement a "significant improvement" over the Privacy Shield, and he referred to part of the redress mechanism consisting in a new Data Protection Review Court. In addition, he detailed the process as one that would take some time—he cited six months of past cases—as from the date that the United States provides first a draft Executive Order (and other relevant acts), then one signed by President Biden, and indicated that perhaps an adequacy decision could be achieved by the end of 2022.[136]

E. Procedure for Adopting a New Adequacy Decision

Not only is there a need to find solutions to existing issues in the recently announced Trans-Atlantic Data Privacy Framework, but there is a procedure to respect once that replacement data agreement is signed. To complete the procedure takes time, as Commissioner Reynders mentioned. The procedure for adopting an adequacy decision following the agreement reached between the DoC and the Commission is set out in Regulation (EU) No 182/2011 (Comitology Regulation),[137] which is referenced in Article 93 of the GDPR on Committee procedure.[138] In this procedure, the Commission's Directorate-General for Justice and Consumers prepares the draft adequacy decision, which is a form of implementing act, and this is submitted to the Article 93 Committee with a draft agenda for a meeting at which it will be discussed. The submission must occur no less than two weeks prior to the meeting, although this period may be shortened in exceptional circumstances. Simultaneously, the draft adequacy decision is made available to the European Parliament and the Council.[139] The Article 93 Committee is made up of Member State representatives and chaired by a Commission representative who does not participate in a vote.[140] Its members may suggest amendments of the adequacy decision and the chair may present amended versions of it, up until the Article 93 Committee delivers an opinion.[141]

---

[135] *See id*. ("The teams of the U.S. Government and the European Commission will now continue their cooperation with a view to translate this arrangement into legal documents…").

[136] Press Conference by Didier Reynders, European Commissioner, on Consumer Rights in the Context of the Green Transition (Mar. 30, 2022), https://audiovisual.ec.europa.eu/en/video/I-222851 [https://perma.cc/992Y-8U6V] (the Commissioner's comments came in response to a question that starts approximately twenty-minutes and forty-five seconds after the start of the video recording).

[137] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 Laying Down the Rules and General Principles Concerning Mechanisms for Control by Member States of the Commission's Exercise of Implementing Powers, 2011 O.J. (L 55) 13 (Feb. 28, 2011) [hereinafter Comitology Regulation] (adequacy decisions are adopted through implementing decisions).

[138] GDPR, *supra* note 5, at art. 93.

[139] Luca Tosoni, *Article 93. Committee Procedure*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 1278, 1283 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey, eds., 2020).

[140] Comitology Regulation, *supra* note 137, at art. 3(2).

[141] *Id*. at art. 3(4).

The Commission must also send the draft to the EDPB, as that body must provide an opinion on its assessment of the adequacy of the data protection involved.[142] In this context, the EDPB indicated its intention to assess carefully "the improvements that a new Trans-Atlantic Data Privacy Framework may bring in the light of EU law, the case-law of the CJEU and the recommendations the EDPB made on that basis," as well as "how these reforms ensure that the collection of personal data for national security purposes is limited to what is strictly necessary and proportionate."[143] Furthermore, the EDPB will examine the redress mechanism of the replacement framework to ensure that it complies with the requirements of the Charter and the CJEU decisions.[144] The EDPB's comments are usually addressed in a refined draft adequacy decision, and a qualified majority vote must be obtained in order for the Article 93 Committee to adopt its opinion in favor of the adequacy decision, in which case the Commission must adopt the adequacy decision.[145] However, when there is a negative opinion, the Commission must either drop the proposal, submit an amended version within two months, or refer the draft to an Appeal Committee within one month, which has the same voting rules as the Article 93 Committee, but is composed of higher rank representatives of Member States—usually ministers.[146] Following a positive opinion, the adequacy agreement is formally adopted by the College of Commissioners and published in the Official Journal, and takes effect on the date indicated in the adequacy decision.[147]

F. Conclusion on a Privacy Shield Replacement

Yet, given the positions of the CJEU in *Schrems I* and *Schrems II*, it appears that the only way to have an EU-U.S. data agreement leading to an adequacy decision that will stand up to a probable new challenge would be to make changes to allow for effective redress against unlawful personal data processing through independent non-executive bodies, although changes to U.S. surveillance legislation may be required.[148] This is the challenge of the new Trans-Atlantic Data Privacy Framework announced in principle. The solution will need to ensure that there is no interference with the essence of the fundamental rights to privacy and to data protection, as such a concept is discussed in Part IV *infra*.

---

[142] GDPR, *supra* note 5, at art. 70(1)(s).

[143] EURO. DATA PROT. BOARD, *Statement 01/2022 on the Announcement of an Agreement in Principle on a New Trans-Atlantic Data Privacy Framework* (Apr. 6, 2022), https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf [https://perma.cc/874A-42LW] [hereinafter *Statement 01/2022*].

[144] *Id*.

[145] *See* Tosoni, *supra* note 139, at 1284.

[146] *Id*. at 1284-86. However, reportedly a negative opinion of Member State representatives is unlikely, "as governments typically prioritize economic and political links with Washington over data protection concerns." Manancourt & Scott, *supra* note 131.

[147] *See* Tosoni, *supra* note 139, at 1286.

[148] *See, e.g.*, Clarke, *supra* note 124.

This will, as mentioned above, take time, and so companies transferring EU personal data to the United States should foresee alternate mechanisms to do so, such as SCCs, also discussed in Part IV, if the conditions for their use are met. As the EDPB stated, "[a]t this stage," the Trans-Atlantic Data Privacy Framework announcement "does not constitute a legal framework on which data exporters can base their data transfers to the United States. Data exporters must therefore continue taking the actions required to comply with the case law of the CJEU, and in particular its Schrems II decision of 16 July 2020."[149]

IV. STANDARD CONTRACTUAL CLAUSES—INTRODUCING THE 2021 EDITION

This Part commences with a brief historical introduction to standard contractual clauses (SCCs). Then, this study investigates the version of the SCCs approved in 2021, following the application of the GDPR and the rendering of the CJEU's *Schrems II* judgment.

A. Brief Historical Introduction to Standard Contractual Clauses

Prior to the adoption and subsequent application of the GDPR, the 1995 Directive provided that the Commission could decide "that certain standard contractual clauses offer sufficient safeguards"[150] to authorize data transfers to third countries not benefitting from an adequacy decision, where those SCCs offered "adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights."[151] The Commission used such power four times under the 1995 Directive, to issue four decisions resulting in three versions of SCCs for two kinds of data transfers; controller-to-controller and controller-to-processor.[152] In June 2001, a decision was issued on SCCs for controller-to-controller transfers,[153] which was amended by a new decision in 2004, providing an alternative version of the SCCs with a different liability regime between the parties, based on due diligence obligations.[154] In late 2001, a decision was issued on SCCs for

[149] *Statement 01/2022*, *supra* note 143.

[150] 1995 Directive, *supra* note 27, at art. 26(4).

[151] *Id*. at art. 26(2).

[152] W. GREGORY VOSS & KATHERINE WOODCOCK, NAVIGATING EU PRIVACY AND DATA PROTECTION LAWS 72 (2015).

[153] Commission Decision of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Directive 95/46/EC, 2001/497/EC, 2001 O.J. (L 181) 19.

[154] Commission Decision of 27 Dec., 2004 Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004/915/EC, 2004 O.J. (L 385) 74.

controller-to-processor transfers,[155] which was repealed and replaced by the SCC Decision in 2010.[156]

In 2016, following the *Schrems I* judgment, an amendment was made to the June 2001 SCC Decision and to the SCC Decision that followed in 2010, to replace language that limited the powers of national supervisory authorities, and to require notice without delay to the Commission if the Member States suspended or banned data flows to third countries pursuant to their powers under Article 28(3) of the 1995 Directive.[157] The *Schrems II* case was based on the SCC Decision and the 2016 amendment. However, all the SCC decisions, as amended, were all still issued under the 1995 Directive and had not been drafted to reflect the provisions of the GDPR.[158]

B. An Investigation of the 2021 Version of the Standard Contractual Clauses

This Section investigates the 2021 Version of the SCCs, intended to modernize the clauses to reflect requirements of the GDPR and the *Schrems II* decision. First, I explain the structure, application, and scope of the 2021 Version of the SCCs. Following that, I study the requirement for an investigation of destination country law of the *Schrems II* judgment. Next, this article tackles the requirement to respect the essence of fundamental rights and freedoms. Then, I examine potential bases for restricting certain GDPR rights and obligations. Finally, this article discusses reasons for terminating the SCC contract or suspending transfers and certain requirements for notifications by the data importer.

1. Structure, Application, and Scope of the 2021 Version of the SCCs

In June 2021, the Commission modernized and replaced the SCC decisions with one new decision (2021 SCC Decision), with four possible modules to choose from,[159] two of which are new, reflecting significant developments in the

---

[155] Commission Decision of 27 Dec., 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, Under Directive 95/46/EC, 2002/16/EC, 2002 O.J. (L 6) 52.

[156] SCC Decision, *supra* note 78.

[157] Commission Implementing Decision (EU) 2016/2297 of 16 Dec., 2016 Amending Decisions 2001/497/EC and 2010/87/EU on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries and to Processors Established in Such Countries, Under Directive 95/46/EC of the European Parliament and of the Council, 2006 O.J. (L 344) 100.

[158] Court of Justice of the European Union Press Release No 91/20, The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield (July 16, 2020).

[159] 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, 2021 O.J. (L 199) 31 (June 7, 2021), recital (10), [hereinafter 2021 SCC Decision] (in this "modular approach," "controllers and processors should select the module applicable to their situation, so as to tailor their obligations under the standard contractual clauses to their role and responsibilities in relation to the data processing in question."). For a critical assessment of the 2021 SCC Decision, *see* W. Kuan Hon, *The 2021 EU SCCs: Practical Issues… & Some Solutions?*, SCL (Jan. 20,

data economy leading to the diversity of conditions today.[160] These four modules are:

Module One: Controller-to-controller transfers;

Module Two: Controller-to-processor transfers;

Module Three: Processor-to-processor transfers (new); and

Module Four: Processor-to-controller transfers (new).[161]

The 2001 and 2010 SCC decisions were both repealed with effect from September 27, 2021,[162] although contracts entered into before that date continued to be effective until December 27, 2021.[163] In adopting the new 2021 SCC Decision, the EU legislators recognized that "Technological developments are facilitating cross-border data flows necessary for the expansion of international cooperation and international trade," however a high level of data protection must be continued after the data are transferred.[164]

Specifically, the 2021 SCC Decision is not available for transfers where the processing by the importer falls under the GDPR, for example, where the importer is subject to the territorial scope of the GDPR under its Article 3(2).[165] Furthermore, onward transfers by a data importer in a third country (or an international organization) to another third country (or an international organization) may only be made if the conditions provided in Chapter V ("Transfers of personal data to third countries or international organizations") of the GDPR are met.[166] In addition, the third party to whom such transfer is made must either accede, or the continuity of data protection is provided otherwise, or in specific situations (derogations), for example, based on explicit, informed data subject consent.[167] Data subjects should be able to act as third party beneficiaries and enforce the SCC's term, except for internal provisions governing the data exporter/data importer relationship.[168]

Importantly, the 2021 SCC Decision sets out requirements for respect of what may be described as the key data protection principles (or data protection safeguards): in controller-to-controller transfers (module one) these include purpose limitation, transparency, accuracy and data minimization, storage limitation, and

---

2022, 4:00 PM), https://www.scl.org/articles/12497-the-2021-eu-sccs-practical-issues-some-solutions [https://perma.cc/XQZ5-YGG9].

[160] *Id*. at recital (6).

[161] 2021 SCC Decision, *supra* note 159 (various provisions for each of the modules or groups of them are detailed throughout the 2021 SCC Decision).

[162] *Id*. at art. 4(2)-(3).

[163] *Id*. at art. 4(4).

[164] *Id*. at recital (1).

[165] *Id*. at recital (7). *See* discussion on territorial scope *supra* Part II.A.

[166] GDPR, *supra* note 5, at art. 44.

[167] 2021 SCC Decision, *supra* note 159, at recital (11), annex module one cl. 8.7, module two cl. 8.8, and module three cl. 8.8.

[168] *Id*. at recital (12).

security of processing, in addition to specific protections for sensitive data.[169] Moreover, the data importer will have to document, inter alia, its processing activities.[170] However, perhaps more interesting are the provisions which reflect the *Schrems II* decision requirements.

2. *Schrems II* Ruling Requirement for an Investigation of Local Laws and Practices of the Destination Country

Under the 2021 SCC Decision, the data exporter warrants that "it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations" under the SCCs.[171] All four modules contain the same clause on "Local laws and practices affecting compliance with the Clauses."[172] In it, the parties:

> warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations" under the SCCs. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.[173]

Article 52(1) of the Charter provides in part that "Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms."[174] The Charter recognizes the rights of privacy (respect for private and family life)[175] and data protection (protection of personal data)[176] as fundamental rights, among others.

---

[169] *See id*. at annex module one cl. 8.1-8.6, module two cl. 8.2-8.7, module three cl. 8.2-8.7, module four cl. 8.2. In the case of transfers to a processor (modules two and three) the reference to accuracy and data minimization has been changed to "accuracy," because it is the controller, and not the processor, which determines the data collected and processed under the GDPR. Furthermore, in the same modules, storage limitation has been changed to "duration of processing and erasure or return of data," to reflect the different role of the processor, as opposed to the controller.

[170] *Id*. at annex modules one, two and three cl. 8.9. In module four annex clause 8.3 the corresponding clause is limited to each party be able to prove compliance and the data exporter providing information to the importer to demonstrate compliance.

[171] *Id*. at annex cl. 8 (this clause is applicable to all four modules).

[172] *Id*. at annex cl. 14.

[173] *Id*. at annex cl. 14(a).

[174] Charter, *supra* note 10, at art. 52(1).

[175] *Id*. at art. 7.

[176] *Id*. at art. 8.

In providing their warranty with respect to local law, the parties will have to investigate the following:

> (1) the specific circumstances of the transfer, including 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; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
>
> (2) the laws and practices of third country of destination—including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
>
> (3) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.[177]

This assessment must be documented and made available to the relevant supervisory authority upon request.[178] Furthermore, the data importer must warrant that in making its assessment it used best efforts to provide the exporter with the relevant information and will cooperate to ensure SCC compliance,[179] and that it agrees to notify the exporter promptly if "it has reason to believe that it is or has become subject to laws or practices not in line with the requirements" of Clause 14(a) of the Annex to the 2021 SCC Decision, "including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements of paragraph (a)."[180] If the data exporter receives such a notification, or if it has reason to believe that the importer can no longer fulfill its obligations, it must promptly identify appropriate measures (such as technical or organizational measures to ensure data security and confidentiality) to correct the situation. If it considers that no such measures can be ensured, or if so ordered by the supervisory authority, it must suspend the data transfer, and may be entitled to terminate the contract using the SCCs.[181]

3. Requirement to Respect the Essence of Fundamental Rights and

---

[177] 2021 SCC Decision, *supra* note 159, at annex cl. 14(b).

[178] *Id*. at annex cl. 14(d).

[179] *Id*. at annex cl. 14(c).

[180] *Id*. at annex cl. 14(e).

[181] *Id*. at annex cl. 14(f).

Freedoms

The concept of respecting the essence of the fundamental rights and freedoms has been discussed in the context of *Digital Rights Ireland*[182] and *Schrems I*, in which cases the CJEU jurisprudence first established the notion of interference with the essence of a fundamental right,[183] in the context of privacy and data protection. In *Schrems I*, for example, U.S. surveillance legislation allowing public authorities electronic communication on a generalized basis compromised the essence of the fundamental right to privacy.[184] The core purpose of the concept is to prevent the holder of the right from being "stripped of the inalienable core of her fundamental right,"[185] or devoiding the right of its content.[186] However, the concept of essentially equivalent protection, which is seen in both *Schrems I* and *Schrems II*, may be a broader one than the essence of a fundamental right, and covers the actual level of protection of EU secondary law,[187] such as the 1995 Directive and the GDPR. Finally, commentators seem to agree that there is some ambiguity in the concept of the essence of fundamental rights and freedoms and that further development by the CJEU will be necessary.[188]

---

[182] Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Comm. Marine & Natural Res. (Apr. 8, 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293&from=en [https://perma.cc/9Y77-PKQ3]. For a short discussion of this case, *see* W. Gregory Voss, *European Union Data Privacy Law Developments*, 70 BUS. LAW. 253, 257-59 (2014).

[183] Maja Brkan, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, 20 GERMAN L.J. 864, 865 (2019).

[184] Schrems I, *supra* note 47, at para. 94. For a short summary of CJEU opinions on the essence of fundamental rights to privacy and data protection, *see* Dominique Moore, *Article 23. Restrictions*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 543, 553 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey, eds., 2020).

[185] Brkan, *supra* note 183, at 866 (adding that there is some differing between Member States on "whether every fundamental right possesses an untouchable core and whether a separate protection of such core is necessary or even appropriate").

[186] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS & COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 44 (2018) ("In the EU legal order, any limitation on the fundamental rights protected under the Charter must respect the essence of those rights. This means that limitations that are so extensive and intrusive so as to devoid a fundamental right of its basic content cannot be justified. If the essence of the right is compromised, the limitation must be considered unlawful, without a need to further assess whether it serves an objective of general interest and satisfies the necessity and proportionality criteria.") [hereinafter HANDBOOK ON EUROPEAN DATA PROTECTION LAW].

[187] Brkan, *supra* note 183, at 882.

[188] *See* Moore, *supra* note 184, at 553 (citing Maja Brkan, *The Concept of the Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core*, 14(2) EUR. CONST. L. REV. 332 (2018)); *see also* Mark Dawson, Orla Lynskey & Elise Muir, *What is the Added Value of the Concept of the "Essence" of EU Fundamental Rights?*, 20 GERMAN L.J. 763, 777 (2019) (synthesizing the issues involved in the introductory article to a special issue of the journal); *see also* Dara Hallinan, *The Essence of Data Protection: Essence as a Normative*

4. Potential Restrictions of Certain GDPR Rights and Obligations

The objectives listed in Article 23(1) of the GDPR and mentioned above, which include possible bases for restricting certain rights and obligations under the GDPR, include: national security; defense; public security; criminal prevention, investigation, detection or prosecution or the execution of criminal penalties; important economic or financial interest of the European Union or an EU Member State; the protection of judicial independence and judicial proceedings; prevention, investigation, detection, and prosecution of regulated profession breaches of ethics; monitoring, inspection or regulatory function connected (even occasionally) to the exercise of official authority in the cases above (except for judicial independence and judicial proceedings); the protection of the data subject or the rights and freedoms of others; and the enforcement of civil law claims.[189] The full list as it appears in this Article of the GDPR is exhaustive.[190] Data subject rights that may be restricted under these limitations include those contained in Articles 12 to 22 and Article 34, and those in Article 5 corresponding to the rights and obligations in Articles 12 to 22.[191] Furthermore, to the extent relevant, the legislative measure should contain specific provisions as to the purposes of the processing, the categories of personal data involved, the scope of the restrictions, the safeguards to prevent abuse or unlawful access or transfer, the specification of the controller, storage periods, risks to the data subjects' rights and freedoms, and the data subject's right to be informed about the restriction, unless prejudicial to its purpose.[192]

As stated in the text extracted from the 2021 SCC Decision above, potential restrictions of GDPR rights and obligations on one of these bases under European Union or Member State law must not only respect "the essence of the fundamental rights and freedoms" but also must be "a necessary and proportionate measure in a democratic society."[193] The latter expression, "means that restrictions need to pass a necessity and proportionality test in order to be compliant with the GDPR," which test should be carried out before the legislation is adopted providing a restriction, and which should be documented.[194] The CJEU applies a "strict necessity" test in its jurisprudence, meaning that the legislative measure cannot exceed that which is strictly necessary to reach the relevant

Pivot, 12(3) EUR. J. L. & TECH. 1, 2 (2021) ("Much scholarly work dealing with the concept, however, bemoans the lack of clarity provided in current EU law." Hallinan defines a methodology to describe the concept of essence as a "normative pivot.").

[189] GDPR, *supra* note 5, at art. 23(1)(a)-(j).

[190] *See* EURO. DATA PROT. BOARD, *Guidelines 10/2020 on Restrictions Under Article 23 GDPR: Version 2.0 9* (Oct. 13, 2021), https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf [https://perma.cc/6RQJ-KCZM] [hereinafter *Guidelines 10/2020*].

[191] GDPR, *supra* note 5, at art. 23(1).

[192] *Id*. at art. 23(2)(a)-(h).

[193] *Id*. at art. 23(1).

[194] *Guidelines 10/2020*, *supra* note 190, at 12.

legitimate objectives.[195] Restrictions should meet the requirements of the Charter and the European Convention on Human Rights,[196] and the jurisprudence of the European Court of Human Rights is relevant in this matter, as a similar test must be carried out for limitations on the right to privacy provided in Article 8 of the Convention.[197] In that jurisprudence, the necessity of addressing a pressing social need, the measure's suitability for a legitimate aim, and the limitation's proportionality are examined.[198]

5. Termination of SCC Contract, Suspension of Transfers, and Notifications by the Data Importer

The SCC contract may be terminated with respect to the processing of personal data after suspension where SCC compliance is not restored within a reasonable time and, in any event, within one month.[199] Also, if the importer is in breach of, or unable to comply with, the SCCs the exporter must suspend the transfer until compliance is ensured or the contract is terminated without prejudice to its ability to identify appropriate measures to correct the situation, as mentioned above.[200] An importer's substantial or persistent breach of the SCCs entitles the exporter to terminate the SCC contract with respect to the processing of personal data,[201] as does the importer's failure to comply with a binding court or supervisory authority decision regarding the importer's obligations under the SCCs.[202] Depending on the relevant module of the SCCs, the data transferred prior to termination of the SCC contract under Clause 16(c) of the Annex to the 2021 SCC Decision must be immediately returned or deleted in its entirety at the exporter's choice (Modules One, Two and Three) or the personal data collected by the exporter in the EU which has been transferred prior to such termination must be deleted in its entirety (Module Four).[203]

The data importer must also notify the exporter if it receives a legally binding public authority request under the laws of the destination country for the disclosure of personal data transferred under the SCCs[204] or if it becomes aware any

---

[195] *Id*.

[196] GDPR, *supra* note 5, at recital (73).

[197] *See* European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8(2), Nov. 4, 1950, 213 U.N.T.S. 221 ("There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and *is necessary in a democratic society* in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." (emphasis added)).

[198] *See* HANDBOOK ON EUROPEAN DATA PROTECTION LAW, *supra* note 186, at 40.

[199] 2021 SCC Decision, *supra* note 159, at annex cl. 16(c)(i).

[200] *Id*. at annex cl. 16(b).

[201] *Id*. at annex cl. 16(c)(ii).

[202] *Id*. at annex cl. 16(c)(iii).

[203] *Id*. at annex cl.16(d).

[204] *Id*. at annex cl. 15.1(a)(i).

direct access to such data by a public authority under the laws of the destination country.[205] If a destination country's laws prohibit such notification, the importer must use and document its best efforts to obtain a waiver of the prohibition.[206] Furthermore, where permissible under the destination country's law, the importer must report on requests received (number, type of data, requesting authority, information as to challenges, etc.).[207] The information described in this paragraph must be kept for the life of the SCC contract and made available to the competent supervisory authority upon request.[208] Moreover, the importer retains the obligation to promptly inform the exporter when it cannot comply with the SCCs.[209]

V. SUPPLEMENTAL MEASURES TO ENSURE DATA PROTECTION AND ALLOW TRANSFERS

After the *Schrems II* invalidation of the Privacy Shield Decision no Commission adequacy decision remains for the United States. Thus, in June 2020, the United States joined a group which includes most countries in the world outside of the EEA—except for those fourteen nations fortunate enough to benefit from an adequacy decision—which are listed in Part II.A. Absent a Commission adequacy decision, a controller or processor may transfer personal data to a third country or an international organization "only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."[210] However, supplementary measures may be used to help fill certain gaps in data protection when appropriate safeguards (such as SCCs or BCRs, among others) do not achieve equivalence with GDPR standards.[211]

The concept of supplementary measures is introduced in Section A, prior to an evocation of the assessment of transfer tools in Section B. Then supplemental measures including contractual commitments and technical measures are discussed, respectively, in Section C and Section D of this Part V.

A. Introduction to Supplementary Measures

The CJEU in *Schrems II* recognized that SCCs, which were in question in that case, might not be adequate to protect EU data subjects' personal data, and that "supplementary measures," might be required:

> [T]he standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) [of the GDPR] are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers

---

[205] *Id*. at annex cl. 15.1(a)(ii).

[206] *Id*. at annex cl. 15.1(b).

[207] *Id*. at annex cl. 15.1(c).

[208] *Id*. at annex cl. 15.1(d).

[209] *Id*. at annex cl. 15.1(e); *see also id*. at annex cl. 16(a).

[210] GDPR, *supra* note 5, at art. 46(1).

[211] *See* Schrems II, *supra* note 13, at para. 133.

> and processors established in the European Union and, consequently, independently of the level of protection guarantee in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level required under EU law, they may require, depending on the prevailing position in a particular country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.[212]

Failing to provide such supplementary measures when needed could lead to the suspension or termination of data transfers.[213] The Court did not indicate which supplementary measures would be needed, but data protection authorities and the EDPB helped provide information here. The GDPR and the CJEU do not define "supplementary measures," "additional safeguards," or "additional measures;"[214] however, on November 10, 2020, the EDPB issued a version of its recommendations for supplementary tools for public consultation.[215] The recommendations were finalized in Version 2.0 and adopted on June 18, 2021.[216]

The measures taken to ensure the protection of personal data following transfer to a third country, such that data subject rights are available and enforceable and that legal remedies are available and effective, will largely be determined by analysis done by the data exporter, as detailed in Section B. In that Section, the subject of the European Essential Guarantees for surveillance measures is raised. Such analysis may lead to the conclusion that supplementary measures described in Sections C and D must be provided.

B. Assessment of Effectiveness of Transfer Tools in the Destination Third Country

This first thing this study discusses in connection with supplementary measures are not the supplementary measures mentioned in the *Schrems II* judgment, but the means to identify when and where those supplementary measures are needed to ensure that transfer tools provide an effectively equivalent level of data protection for transfers. As the EDPB indicates, it is up to the data exporter (whether a controller or a processor) to make an assessment and to select

---

[212] *Id*.

[213] *Id*. at para. 135.

[214] EURO. DATA PROT. BOARD, *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data: Version 2.0*, at 8 (June 18, 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [https://perma.cc/A9VT-E6XP] [hereinafter *Recommendations 01/2020 V.2*].

[215] EURO. DATA PROT. BOARD., *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data* (Nov. 10, 2020), https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf [https://perma.cc/QX76-ZR4R].

[216] *Recommendations 01/2020 V.2*, *supra* note 214.

supplementary measures and to document this, with the resulting documentation made available for the competent supervisory authority upon its request.[217]

If an adequacy decision for the third country is available, no specific authorization is required.[218] However, if the basis for a transfer is a transfer tool, then an assessment of its effectiveness in the destination third country must be made and, depending on the result, on a case-by-case basis, supplementary measures may be called for.[219] Transfer tools available include SCCs, BCRs, codes of conduct, certification mechanisms and ad hoc contractual clauses,[220] although SCCs are by far the most popular.[221] In certain circumstances, derogations provided by the GDPR may apply to allow cross-border transfers, however these must be "exceptional" and not "the rule" in practice,[222] thus reducing their interest in the context of multinational enterprises with large-scale transfers.

The EDPB sets out a "roadmap" with steps for assessing whether supplementary measures are necessary to allow data transfers. The steps are as follows:

> Step 1: "Know your transfers;"[223]
>
> Step 2: "Identify the transfer tools you are relying on;"[224]
>
> Step 3: "Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer;"[225]
>
> Step 4: "Adopt supplementary measures;"[226]
>
> Step 5: "Procedural steps if you have identified effective supplementary measures;"[227] and
>
> Step 6: "Re-evaluate at appropriate intervals."[228]

Perhaps the most interesting of these steps for the purposes of this study is step 3. It involves a kind of limited due diligence investigation of the impact of local legislation in the destination country on the effectiveness of the relevant transfer tool. During this step the data exporter must assess, with assistance of the data importer, where appropriate, if the third country's laws or practices

---

[217] *Id*. at 10.

[218] GDPR, *supra* note 5, at art. 45(1). The EDPB cautions, "However, you must still monitor if adequacy decisions relevant to your transfers are revoked or invalidated." *Recommendations 01/2020 V.2*, *supra* note 214, at 12 (citations omitted).

[219] For an example of SCCs, *see* Schrems II, *supra* note 13, at para. 133 and discussion *supra* Part V.A.

[220] *Recommendations 01/2020 V.2*, *supra* note 214, at 13.

[221] *See* Schrems II Impact Survey Report, *supra* note 72, at 5 and accompanying text.

[222] *Recommendations 01/2020 V.2*, *supra* note 214, at 13. The potential derogations are set out in GDPR, *supra* note 5, art. 49(1).

[223] *Recommendations 01/2020 V.2*, *supra* note 214, at 10-11.

[224] *Id*. at 11-13.

[225] *Id*. at 14-21.

[226] *Id*. at 21-23.

[227] *Id*. at 23-25.

[228] *Id*. at 25.

hamper the effectiveness of the safeguards of the relevant transfer tool with respect to the transfer being evaluated. Elements contained in the assessment could include those on "whether public authorities of the third country of your importer may seek to access the data with or without the data importer's knowledge, in light of legislation, practice and reported precedents" and whether such public authorities "may be able to access the data through the data importer or through the telecommunications providers or communications channels in light of legislation, legal powers, technical, financial, and human resources at their disposal and of reported precedents."[229]

Obviously, the rule of law situation in the destination country may be relevant to this analysis.[230] Sources of information relied upon for the assessment should be "relevant, objective, reliable, verifiable and publicly available or otherwise accessible," and you must document that they are so.[231] While the analysis must first be based on legislation in the destination country, the practices of public authorities may indicate that they do not normally comply or apply such legislation, and this must be taken into account. Furthermore, incompatible practices in the destination country may prevent the effectiveness of the transfer tool, which would also need to be considered. Finally, legislation may be found to be problematic, leading to a decision to suspend transfers or implement supplementary measures,[232] such as those discussed in Sections C and D. The EDPB defines "problematic legislation" as follows:

> [L]egislation that 1) imposes on the recipient of personal data from the European Union obligations and/or affect the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognised by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in Union or EU Member States' law, such as those listed in Article 23(1) GDPR.[233]

The concept of essence of fundamental rights and freedoms mentioned in this definition is developed in Part IV.B.3 *supra*.

In relation to interferences with the fundamental rights to privacy and data protection created by surveillance measures, the Article 29 Data Protection Working Party set out European Essential Guarantees (EEG), identified through relevant CJEU and European Court of Human Rights jurisprudence, which must be respected in order for such interferences to be justifiable.[234] These EEG,

---

[229] *Id*. at 14.

[230] *Id*. at 16.

[231] *Id*. at 18.

[232] *Id*. at 17.

[233] *Id*. at 22 n.63.

[234] EURO. DATA PROT. BOARD, *Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures 4*, Nov. 10, 2020,

which are relevant to the assessment of a transfer tool,[235] were originally written in response to the *Schrems I* decision,[236] and are: "A. Processing should be based on clear, precise and accessible rule"; "B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated"; "C. An independent oversight mechanism should exist"; and, "D. Effective remedies need to be available to the individual."[237] Furthermore, the EDPB underscores that these EEG "are based on … fundamental rights … that apply to everyone, irrespective of their nationality."[238] Either the destination third country legislation fulfills these EEG, or it does not ensure them, in which case the country's surveillance measures would fail the test for the justifiability of the interference with fundamental rights. However, the Article 29 Data Protection Working Party noted that the EEG:

> should be seen as the essential guarantees to be found in the third country when assessing the interference, entailed by a third country surveillance measures, with the rights to privacy and data protection, rather than a list of elements to demonstrate that the legal regime of a third country as a whole is providing an essentially equivalent level of protection.[239]

The surveillance measures evaluated in the *Schrems II* case and discussed in Part II.B., for example, failed the EEG test with respect to several points, notably as they were not sufficiently limited nor subject to effective redress for data subjects to enforce their rights,[240] corresponding to a failure to ensure guarantees B and D.

Thus, legislation in the destination country may be problematic, including in instances where the EEG are not ensured with respect to surveillance measures. In such a case, the data exporter, in cooperation with the data importer, will need to determine whether supplementary measures, when cumulated with the transfer tool, will help ensure that the data transferred are provided an essentially equivalent level of protection to that guaranteed in the European Union.[241] This study now examines certain supplementary measures, first, other contractual commitments, then, technical measures such as encryption, and, finally, organizational measures.

---

https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf [hereinafter *Recommendations 02/2020*].

[235] *Recommendations 01/2020 V.2*, *supra* note 214, at 16.

[236] *Recommendations 02/2020*, *supra* note 234, at 5.

[237] *Id*. at 8.

[238] *Id*.

[239] *Id*. at 6.

[240] *Id*. at 5 (The Schrems II "judgment can thus serve as an example where surveillance measures in a third country (in this case the U.S. with Section 702 FISA and Executive Order 12 333) are neither sufficiently limited nor object of an effective redress available to data subjects to enforce their rights…").

[241] *Recommendations 01/2020 V.2*, *supra* note 214, at 21.

C. Other Contractual Commitments

Specifically mentioned by the CJEU in *Schrems II* as additional safeguards to help ensure protection of EU data subjects' personal data are contractual commitments, to the extent they do not contradict SCCs or prejudice data subjects' fundamental rights: "Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses."[242] Such contractual commitments may involve requiring identified technical measures to be used in order for a transfer to occur.[243] They may also be used to impose transparency obligations on the importer, perhaps being detailed in annexes to the contract. Examples of these might include clauses requiring the importer to enumerate applicable laws in the country of destination allowing public authorities access to the personal data, or to disclose details of access requests (or give information on being legally prohibited from doing so), or to indicate what is being done to prevent access.[244] Another suggested contractual commitment is to have the data importer certify that it has not used computer programming to allow access to personal data or the system (such as through back doors) and is not required by law or government policy to do so, or to hand over any encryption key, when applicable.[245]

The contract could also stipulate that the data exporter may conduct audits and inspections of the importer's data processing facilities. Also, if the destination country's laws or practice change in a way that prevents compliance, the importer could be required to return or delete data and the contract would be terminated within a specified period.[246] In addition, a contract may outline a "Warrant Canary" procedure, whereby the importer has an obligation to certify at certain intervals that as of the time of certification the importer has not received any order to hand over personal data.[247] Furthermore, an importer could "commit to reviewing" and challenging orders to disclose data that appear to be based upon unfounded legal assertions.[248] Finally, in cases where importers are asked to voluntarily cooperate with public authorities, a contract could stipulate that personal data "may only be accessed with the express or implied agreement of the exporter and/or the data subject."[249]

However, contractual measures between public authorities and importers, generally only bind public authorities that are parties to the contract.[250] Therefore, although contractual measures provide some protections, they do not shield importers from the laws of countries that are not parties to a contract, even if

---

[242] Schrems II, *supra* note 13, at para. 109.

[243] *Recommendations 01/2020 V.2*, *supra* note 214, at 36-37.

[244] *Id*. at 37.

[245] *Id*. at 38.

[246] *Id*. at 39.

[247] *Id*. at 40 (noting that this could be achieved using a "cryptographically signed message" published "at least every [twenty-four] hours").

[248] *Id*. at 40-41.

[249] *Id*. at 42.

[250] *Id*. at 36.

these "third country" laws do not meet the EEG standard.[251] Thus, the EDPB cautions that "contractual and organisational measures alone will generally not" suffice when data access by public authorities is "based on problematic legislation and/or practices."[252] In those cases, the EDPB recommends that technical measures be relied upon as well.[253]

D. Technical Measures: Encryption and Pseudonymization

Shortly after the CJEU issued the *Schrems II* decision, several Data Protection Authorities ("DPAs") addressed the issue of supplementary measures. The DPA of the German region of Baden Württemberg was among the first to address this topic, by introducing encryption, anonymization, and pseudonymization of data as additional safeguards for personal data transfers to the United States.[254] With respect to encryption, the DPA of Baden Württemberg emphasized that the data exporter should be the sole holder of the encryption key and argued that the encryption should be strong enough to prevent American intelligence services from bypassing the encryption and accessing the data transferred.[255] With respect to pseudonymization, the DPA of Baden Württemberg asserted that only the exporter should have the capability to link the data subject to the personal data.[256]

In its recommendations, the EDPB outlines cases that exemplify effective technical measures, such as preventing public authorities from identifying data subjects or obtaining information about them (including through inference or cross-referencing databases).[257] However, it is ultimately up to the exporter to analyze a particular situation (and with the cooperation of the importer) determine which technical measures are appropriate for a given set of circumstances depending on the laws and practices of the destination country.[258] Although the propriety of technical measures may vary based upon different circumstances,[259]

---

[251] *Id*. at 36 ("[C]ontractual measures will not be able to rule out the application of the legislation of a third country which does not meet the EDPB European Essential Guarantees standard in those cases in which the legislation obliges importers to comply with the orders to disclose data they receive from public authorities.").

[252] *Id*. at 22.

[253] *Id*. at 22 ("Indeed there will be situations where only appropriately implemented technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes.").

[254] *German DPA Issues Guidance on Data Transfers Following Schrems II*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Sept. 2, 2020), https://www.huntonprivacyblog.com/2020/09/02/german-dpa-issues-guidance-on-data-transfers-following-schrems-ii/ [https://perma.cc/KAQ2-W2PW].

[255] *Id*.

[256] *Id*.

[257] *Recommendations 01/2020 V.2*, *supra* note 214, at 31-32, 34.

[258] *Id*. at 29.

[259] *Id*. at 14-15.

in general, technical measures, largely hinge upon the use of encryption and pseudonymization.[260]

If "[a] data exporter uses a hosting service provider in a third country to store personal data" an exporter should implement strong (state-of-the-art) encryption before the data are transmitted.[261] When an exporter uses a "hosting service provider in a third country," the data exporter should retain sole control of data encryption keys or give the encryption keys to "an entity trusted by the exporter" that is located in the EEA or another country that offers "an essentially equivalent level of [data] protection to that guaranteed within the EEA."[262] Pseudonymizing data before transmission may also provide data protection by processing data in a way that prevents the data from being "attributed to a specific data subject."[263] For data pseudonymization to be an effective supplementary technical measure, additional information required to reconnect the data to a specific data subject should be "held exclusively by the data exporter and kept separately . . . by an entity trusted by the exporter" that is located in the EEA or in another country that offers "an essentially equivalent level of [data] protection to that guaranteed within the EEA."[264] Furthermore, technical and organizational safeguards should be used to prevent "disclosure or unauthorized use of [ ]additional information" required to re-identify data subjects and the exporter should maintain "sole control of the algorithm or repository that enables re-identification using [such] information." Finally, the controller should ensure that data cannot be attributed to a data subject by public authorities, "even if cross-referenced" with information that public authorities "may be expected to possess and use."[265]

In addition to encryption and pseudonymization, there are other technical supplementary measures. For example, exporters can split personal data to ensure that no information that "an individual processor receives [is] suffic[ient] to [partially or completely] reconstruct the personal data."[266] When personal data are split, separate processors in different jurisdictions process the different parts.[267] Alternatively, entities can "process [. . .] data jointly," using what the EDPB refers to as "secure multi-party computation."[268] Joint processing may be done in a way that restricts the information that processors receive to information that the processors possessed "prior to the computation."[269]

---

[260] *See id*. at 31-33.

[261] *Id*. at 30.

[262] *Id*.

[263] *Id*. at 31.

[264] *Id*.

[265] *Id*.

[266] *Id*. at 33.

[267] *Id*.

[268] *Id*. at 34.

[269] *Id*.

E. Organizational Measures

Organizational measures can also serve as supplemental measures to help ensure the necessary level of data protection when exporters transfer personal data to a third country. According to the EDPB, organizational measures that promote data protection include "internal policies, organisational methods, and standards [that] controllers and processors could apply to themselves" and require importers to follow.[270] The EDPB highlights internal policies that govern data transfer obligations as an organizational measure that is especially pertinent to data transfers between groups of enterprises.[271] The EDPB also highlights "transparency and accountability measures;" "organisation methods and data minimisation measures;"[272] and "data security and data privacy policies, based on . . . standards . . . and best practices" as supplemental organizational measures that provide data protection.[273] The EDPB cites ISO norms as an example of a standard that may form the basis of a data security or data privacy policy, and ENISA's guidelines as a source of best practices.[274] When data are transferred there are many ways in which data are processed (e.g., through transmission).[275] It is the controller's responsibility to ensure that "appropriate technical and organisational measures" are employed to ensure GDPR compliance,[276] and the controller and processor must "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."[277] ENISA, which is now named the European Union Agency for Cybersecurity,[278] has been working to create guidelines and provide best practices, which help determine the appropriate level of action required for security purposes.[279]

Now that this study has shown how to determine whether supplementary measures are required for cross-border transfers of personal data to third countries which have not benefitted from a Commission adequacy decision, and what constitutes potential supplementary measures, it now illustrates with certain GDPR enforcement actions involving transfers, whether those have resulted in a sanction or are still in process.

---

[270] *Id*. at 43.

[271] *Id*. at 43-44.

[272] *Id*. at 44-45.

[273] *Id*. at 45-46.

[274] *Id*. at 46.

[275] See GDPR *supra*, note 20 for the GDPR definition of "processing."

[276] GDPR, *supra* note 5, at 47.

[277] *Id*. at 51-52.

[278] ENISA, *About ENISA - The European Union Agency for Cybersecurity*, ENISA, https://www.enisa.europa.eu/about-enisa [https://perma.cc/34EL-YRUQ].

[279] *See, e.g.*, W. Gregory Voss, *The Concept of Accountability in the Context of the Evolving Role of ENISA in Data Protection, ePrivacy, and Cybersecurity*, TECHNOCRACY AND THE LAW: ACCOUNTABILITY, GOVERNANCE AND EXPERTISE 256 (Alessandra Arcuri & Florin Coman-Kund, eds., 2021).

VI. EEA ENFORCEMENT ACTIONS INVOLVING CROSS-BORDER TRANSFERS

Very few EEA enforcement actions involving a violation of the cross-border transfer provisions of the GDPR have resulted in administrative fines issued to the controller or the processor. A search on the CMS.Law GDPR Enforcement Tracker for sanctions involving a violation of one or more of Articles 44 through 49 of the GDPR, which are all but one of the articles constituting its Chapter V (Transfers of personal data to third countries or international organisations), showed only four violations,[280] discussed in Sections one through four below. The cause of this paucity of sanctions is a subject for further research, although one potential reason may be related to the slowness of the Irish supervisory authority in completing enforcement action against U.S. Big Tech firms.[281] The Irish regulator—the Data Protection Commission (DPC)—acts as lead supervisory authority under the "one-stop-shop" mechanism[282] with respect to many U.S. technology companies who have their main EU establishment in Ireland,[283] as is the case for Facebook (Meta), which is the primary focus in Section B. Finally, a related action by the European Data Protection Supervisor is detailed in Section C.

This study first summarizes Member State supervisory authority administrative fines issued in actions involving cross-border transfers, before discussing the situation in Ireland, particularly insofar as Facebook (Meta) is concerned, in addition to an enforcement case brought by the European Data Protection Supervisor.

A. Member State Supervisory Authority Administrative Fines

Under the GDPR several paths exist for sanctioning data protection violations, perhaps the most emblematic of which is the issue of administrative fines by Member State supervisory agencies, which must be "effective, proportionate and dissuasive."[284] This study surveys Member State supervisory authority

---

[280] CMS.Law GDPR Enforcement Tracker, whose creator is enforcementtracker.com, provided by CMS Law.Tax, CMS.LAW GDPR ENFORCEMENT TRACKER, https://www.enforcementtracker.com [https://perma.cc/7TG5-2CWP] (A search for the numbers for Articles 44 through 49 of the GDPR was conducted under the column "Quoted Art." on each page of the website).

[281] *See, e.g.*, W. Gregory Voss & Hugues Bouthinon-Dumas, *EU General Data Protection Regulation Sanctions in Theory and in Practice*, 37 SANTA CLARA HIGH TECH. L.J. 1, 92 (2021) (Discussing the then "failure to date of the Irish DPA to bring to completion enforcement action against the U.S. Tech Giants.") [hereinafter Voss & Bouthinon-Dumas].

[282] GDPR, *supra* note 5, at art. 56. This "one-stop-shop" mechanism is described in Voss & Bouthinon Dumas, *supra* note 281, at 60-63.

[283] *See*, *e.g.*, Voss & Bouthinon-Dumas, *supra* note 281, at 70.

[284] GDPR, *supra* note 5, at art. 83(1). For a discussion of Member State supervisory agencies fines issued under the GDPR generally, *see* Josephine Wolff & Nicole Atallah, *Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020*, 11 J. INFO. POL'Y 66 (2021); *see also* Mona Naomi Lintvedt, *Putting a Price on Data Protection Infringement*,

administrative fines from France, Spain, Italy, Norway, and Austria for data protection violations involving the cross-border transfer provisions of the GDPR.

1. France—Futura Internationale

On November 21, 2019, prior to the *Schrems II* decision, the Futura Internationale company was issued an administrative fine of €500,000 by the French supervisory authority (Commission nationale informatique et libertés (CNIL)), in part based on a violation of Article 44 of the GDPR.[285] Following a formal demand by the CNIL, Futura established contractual clauses as the basis for its transfer of personal data to subcontractors in third countries not benefiting from a Commission adequacy decision (Ivory Coast, Morocco, and Tunisia, using its Progibos software[286]) for telephone prospecting campaigns but failed to use SCCs adopted by the Commission or a Member State supervisory authority.[287]

During the sanctioning procedure, Futura adopted clauses from the SCCs, however the clauses presented were neither in final form nor fully drafted, in particular the remuneration clause, and were not signed by the two parties.[288] Furthermore, while the contracts were subject to the choice of the law of the nation of the subcontractor, the choice of law should have indicated the law of the Member State of the data exporter—France.[289] The CNIL ordered that legal acts between Futura and its subcontractors meeting the criteria laid down in Articles 44 to 49 of the GDPR had to be established, and if Futura chose to use SCCs adopted by the Commission, these had to be signed by the parties and governed by the law of the Member State in which the data exporter is established, which is France.[290] This case was appealed up to the French Council of

12 INT'L DATA PRIVACY L. 1 (2022), https://academic.oup.com/idpl/article/12/1/1/6453860; and *see* Voss & Bouthinon-Dumas, *supra* note 281.

[285] *See* Commission Nationale de l'Informatique et des Libertés, *Délibération de la formation restreinte n°SAN-2019-010 du 21 novembre 2019 concernant la société X* (Deliberation of the Sanctions Committee of the CNIL No. SAN-2019-010 Concerning Company X), https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000039419459/ [https://perma.cc/Z89E-4UZS] [hereinafter Futura]. Note that the CNIL anonymizes its decisions two years after publication, as indicated in its decision, but this case is indicated as relating to Futura Internationale at reference (ETid-118) by CMS.LAW GDPR ENFORCEMENT TRACKER, *supra* note 280. A summary and a machine translation of this decision are also provided at *CNIL - SAN-2019-010*, GDPRHUB, https://gdprhub.eu/index.php?title=CNIL_-_SAN-2019-010 [https://perma.cc/LVR8-P32H].

[286] *See* Futura, *supra* note 285, para. 73.

[287] *Id*. at para. 75.

[288] *Id*. at paras. 76-79.

[289] *Id*. at para. 80.

[290] *Id*. ("La formation restreinte de la CNIL, après en avoir délibéré, décide de: … d'encadrer les relations entre la société et ses sous-traitants procédant aux campagnes de prospection téléphonique par des actes juridiques répondant aux critères posés par les articles 44 à 49 du Règlement et de s'assurer, si la société fait le choix des clauses types de protection des données adoptées par la Commission européenne, que les clauses sont signées par les parties et

State (*Conseil d'État*), France's highest administrative court, and Futura Internationale sought to have the fine annulled or significantly reduced. The Council of State dismissed Futura Internationale's claims and confirmed that the fine, which was in an amount equal to 2.5% of Futura Internationale's annual turnover, was not excessive.[291]

This case is interesting because it involves the export of data for processing to countries other than the United States, which are low-cost destinations for sub-contracting. It also highlights the need for good administration of transfer tools, which in this case was sorely lacking. Finally, the significant percentage of annual revenue fined is notable (as a reminder, the maximum under the GDPR is 4%).

2. Spain—Vodafone España

On March 11, 2021, the Spanish supervisory authority—Agencia Española de Protección de Datos (AEPD)—issued a fine of €8,150,000 against Vodafone España, S.A.U. in part for violation of Article 44 of the GDPR (specifically assessing €2,000,000 of the total for that).[292] Vodafone entered a contract with Casmar for the processing of the personal data in Peru, by which the latter would carry out the work through a subcontractor—A-Nexo.[293] No safeguards for such transfer were provided, contrary to what is required by Chapter V of the GDPR,[294] as Vodafone transferred personal data to a third country (here, Peru) which does not benefit from a Commission adequacy decision.

This case is clear cut, and just emphasizes that companies must understand their legal obligations under the GDPR.

---

régies par le droit de l'État membre dans lequel l'exportateur de données est établi, en l'espèce la France").

[291] CE, 10ème – 9ème ch. réuns., Mar. 1, 2021, 437808, https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043205058 [https://perma.cc/A6GP-CS3D] (unpublished opinion). The ruling on this appeal is summarized in English at *CE – 437808*, GDPRHUB, https://gdprhub.eu/index.php?title=CE_-_437808 [https://perma.cc/A3RX-7H7H].

[292] AEPD (Agencia Española de Protección de Datos) [Spanish Data Protection Agency], Mar. 11, 2021 (Procedimiento Sanctionador N° PS/00059/2020 [AEPD Sanctioning Procedure No. PS/00059/2020]), https://www.aepd.es/es/documento/ps-00059-2020.pdf [https://perma.cc/947D-JES5] [hereinafter Vodafone]. A summary of this case and a machine translation of it are provided in English at *AEPD - PS/00059/2020*, GDPRHUB, https://gdprhub.eu/index.php?title=AEPD_-_PS/00059/2020 [https://perma.cc/N4KC-E8CK]. *See also Spain: AEPD fines Vodafone Spain €8.15M for commercial communication failures*, ONETRUST DATAGUIDANCE (Mar. 12, 2021), https://www.dataguidance.com/news/spain-aepd-fines-vodafone-spain-%E2%82%AC815m-commercial [https://perma.cc/X8PR-DHWS].

[293] Vodafone, *supra* note 292, at § 6R: Respecto al incumplimiento del artículo 44 del RGPD, at 64.

[294] *See id*. at 64, 79.

3. Italy—Bocconi University

In September 2021 a case involving cross-border transfers resulted in sanctions against Bocconi University (Università Commerciale "Luigi Bocconi" di Milano) in Italy in part for having transferred personal data to a third country--the United States--without having proven to have verified and ensured that the transfer in question was carried out in effective compliance with the conditions set out in Chapter V of the GDPR, in violation of its Articles 44 and 46.[295] The case involved the University's use of software from Respondus Inc. (Respondus Monitor) for proctoring exams, ostensibly used in order to prevent student fraud during online exams administered during the COVID-19 pandemic. In this context, biometric data (considered sensitive data under the GDPR) were used to identify students.[296]

Respondus, which was the data processor, had used the Privacy Shield Decision as the basis for data transfers to the United States.[297] Following the *Schrems II* decision, the University added standard contractual clauses to the contract with Respondus, in an amendment to the data protection agreement in August 2020. However, in this document, the processor Respondus did not provide the guarantee of technical and organizational measures required under the referenced SCCs, and security measures were not detailed in the clauses as they should have been, thereby depriving data subjects of guarantees with respect to which they were third party beneficiaries. Also, the documentation did not show any additional measures adopted to ensure compliance with the required level data protection, nor any evidence of an assessment of this by the University. The same considerations also applied to the transfer to the sub-processor, Amazon Web Services Inc., also established in the United States. In addition, it appears that data were only encrypted after processing by the processor, so were transferred in the clear.[298]

As a result, the supervisory authority ordered a halt to the contested processing through the Respondus system and issued an administrative fine of €200,000 with respect to violations of Articles 5(1)(a), (c) and (e), 6, 9, 13, 25, 35, 44 and 46 of the GDPR.[299] This case underscores the importance of

---

[295] Garante per la Protezione dei Dati Personali [Guarantor for the Protection of Personal Data], 16 settembre 2021, Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano [9703988] [Injunction order against the "Luigi Bocconi" Commercial University of Milan [9703988]], https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9703988 [https://perma.cc/D47V-RYWZ]. (This decision is based on a violation of several articles of the GDPR—Articles 5(1)(a), 5(1)(c), 5(1)(e), 6, 9, 13, 25, 35—in addition to Articles 44 and 46).

[296] *Id*.

[297] *Id*. ("[I]l Trattamento comporta un trasferimento dei dati extra UE da parte del Fornitore" che ha dichiarato di essere "conforme al Privacy Shield Framework EU -U.S.").

[298] *Id*.

[299] *Id*. For a summary and machine translation in English of this case, *see Garante per la protezione dei dati personali (Italy) – 9703988*, GDPRHUB,

providing the necessary level of security for the data being transferred and following EDPB recommendations on supplemental measures.

4. Norway--Ferde

In another September 2021 case, the Norwegian supervisory authority (Datatilsynet) fined Norwegian toll company Ferde AS five million Norwegian krone (approximately €500,000[300]) for, among other things, transferring personal data to China for processing without a valid legal basis under the GDPR, in violation of its Article 44,[301] as no transfer mechanism was in place. This transfer outside of the EEA was made to a country—China—that does not benefit from a Commission adequacy decision.

Datatilsynet determined that Ferde AS failed to establish a data processing agreement and did not carry out a risk assessment. However, the criteria from the *Schrems II* decision were not considered, as the period investigated (September 2017—October 2019) preceded that ruling.[302] Nonetheless, this case is significant in that it involves data transfer not to the United States, but to China, which also houses many large technology firms, and could be used as a low-cost destination for sub-contracting processing, much like the destination countries in the French case discussed in Section 1.

5. Austria—NetDoktor

Perhaps the most interesting in many respects of these Member State cases is one from the Austrian supervisory authority Datenschutzbehörde (DSB), which found an unnamed German publisher to be in violation of Article 44 of the GDPR in the publisher's use of Google Analytics and its transfer of personal data to the United States, although no fine has been issued so far.[303] Google hosts

---

https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9703988 [https://perma.cc/9TUF-N4SU].

[300] *The Norwegian Data Protection Authority: Ferde AS fined*, EURO. DATA PROT. BOARD (Oct. 13, 2021), https://edpb.europa.eu/news/national-news/2021/norwegian-data-protection-authority-ferde-fined_en [https://perma.cc/2WFE-U8HL].

[301] "The Data Protection Authority's investigation has revealed that Ferde AS had failed to both establish a data processing agreement and to carry out a risk assessment and also lacked a legal basis for the processing of personal data about motorists in China. These are all basic responsibilities under relevant data protection legislation, and these requirements must be met before the processing of personal data can take place." *Ferde AS fined*, DATATILSYNET (Oct. 6, 2021), https://www.datatilsynet.no/en/news/2021/ferde-as-fined/ [https://perma.cc/VQG5-3CTH].

[302] Additional details of this case and an English machine language translation of the decision are available at *Datatilsynet (Norway) - 20/01727*, GDPRHUB, https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/01727 [https://perma.cc/XF2S-463E].

[303] Lindsay Clark, *Austrian Watchdog Rules German Company's Use of Google Analytics Breached GDPR by Sending Data to US*, REGISTER (Jan. 13, 2022, 14:48 UTC), https://www.theregister.com/2022/01/13/google_analytics_gdpr/ [https://perma.cc/9N4K-VZ7R].

the data in the United States, where they are stored and further processed.[304] The case involves Googles Analytics cookies placed on the Austrian medical news website NetDoktor, which track visitor interaction with the site, collect information about the user's device, and potentially link to other data using a Google identification number associated with the user's browser.[305] Here, the SCCs used were not sufficient to comply with the GDPR, as Google may be subject to surveillance under FISA 702, and technical and organizational measures provided (which included "baseline encryption") were not sufficient, as they did not eliminate the possibility of access by U.S. public authorities.[306] Apparently, Google, which based the transfer of personal data to the United States on SCCs,[307] could access data in plain text, meaning they were not protected from such surveillance.[308] Nonetheless, the DSB found that the GDPR only placed legal duties on the data exporter (the publisher) and not on the importer (Google LLC), although it announced it would conduct an investigation regarding the latter's compliance with GDPR Articles 5, 28(3)(a) and 29.[309]

This decision is likely to be followed by many similar ones from various Member State supervisory authorities as NOYB has filed 101 complaints across the European Union against companies using Google Analytics[310] after the *Schrems II* decision. For example, the Netherlands data protection supervisory authority (Autoriteit Persoonsgegevens (Dutch DPA)) has reportedly been investigating two cases involving the use of Google Analytics and has announced "the use of Google Analytics may soon not be allowed."[311] The Norwegian data authority has advised firms to investigate alternatives to Google services,[312] as has the Liechtenstein data authority.[313] Although no fine has been issued yet,

---

[304] Oliver Noyan, *Use of Google Analytics Violates EU Law, Austrian Authority Rules*, EURACTIV (Jan. 13, 2022), https://www.euractiv.com/section/politics/short_news/use-of-google-analytics-violates-eu-law-austrian-authority-rules/ [https://perma.cc/CL42-WYEH].

[305] *See* Burgess, *supra* note 125.

[306] *See* Clark, *supra* note 303.

[307] *See DSB (Austria) - 2021-0.586.257 (D155.027)*, GDPRHUB, https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2021-0.586.257_(D155.027) [https://perma.cc/FW3W-8MV6].

[308] *See* Burgess, *supra* note 125.

[309] *See* GDPRHUB, *supra* note 307.

[310] Clark, *supra* note 303.

[311] Jennifer Bryant, *Austrian DPA's Google Analytics Decision Could Have 'Far-reaching Implications'*, IAPP (Jan. 20, 2022), https://iapp.org/news/a/far-reaching-implications-anticipated-with-austrian-dpas-google-analytics-decision/ [https://perma.cc/RXT8-4AKK].

[312] Vincent Manancourt & Laura Kayali, *US-EU Data Transfers on Life Support After French Google Decision*, POLITICO (Feb. 10, 2022, 2:12 PM), https://www.politico.eu/article/us-eu-data-transfers-on-life-support-after-french-google-decision/ [https://perma.cc/4H59-HYUQ].

[313] *Leichtenstein: DSS Addresses Use of Google Analytics*, DATA GUIDANCE (Mar. 3, 2022), https://www.dataguidance.com/news/liechtenstein-dss-addresses-use-google-analytics%C2%A0 [https://perma.cc/9WBK-THJ4] ("Notably, the DSS called on affected entities

France's CNIL ordered an unnamed website manager/operator "to comply with the GDPR and, if necessary to stop using this service under the current conditions,"[314] and compiled a list of alternative web audience measurement tools.[315] Previously, the Bavarian data authority called for a German data controller to stop its use of the Mailchimp tool based on cross-border data transfer concerns involving transfers to the United States.[316] Reportedly, supervisory authorities in thirty European nations are investigating other cases covering both Google Analytics and Facebook Connect.[317]

This case raises questions about the use of web tools that transfer data to the United States, such as Google Analytics or cloud services, and has implications for a case involving Facebook in Ireland[318] discussed in Section B.

B. Ongoing Action in Ireland: Facebook (Meta) and Possibly Tik-Tok

In late August 2020, shortly after the *Schrems II* ruling, the Irish DPC sent Facebook a preliminary order to halt transfers of EU data subjects' personal data to the United States, asking for Facebook's response.[319] This marked a sea change in EU-U.S. personal data transfer relations, as the first such order to stop such transfers, and the DPC's reasoning that SCCs were not sufficient under the *Schrems II* ruling could be extended to other technology and telecommunications companies subject to Section 702 of FISA.[320] That section applies to an "electronic communication service provider," which means:

> (A) a telecommunications carrier …,
>
> (B) a provider of electronic communication service …,

---

to design their websites in compliance with the data protection rules and to use alternative, data protection-compliant solutions instead of Google Analytics.").

[314] *Use of Google Analytics and Data Transfers to the United States: the CNIL Orders a Website Manager/Operator to Comply*, CNIL (Feb. 10, 2022), https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply [https://perma.cc/G86Y-CP3N] (Note that "The CNIL has issued other orders to comply to website operators using Google Analytics.").

[315] *Cookies: Solutions pour les Outils de Mesure d'Audience*, CNIL (Sept. 23, 2021), https://www.cnil.fr/fr/cookies-solutions-pour-les-outils-de-mesure-daudience [https://perma.cc/2WXM-UZ6T].

[316] *Bavarian DPA (BayLDA) Calls for German Company to Cease the Use of 'Mailchimp' Tool*, EDPB (Mar. 30, 2021), https://edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool_en [https://perma.cc/2T9M-H98J].

[317] Burgess, *supra* note 125.

[318] *See* Natasha Lomas, *In Bad News for US Cloud Services, Austrian Website's Use of Google Analytics Found to Breach GDPR*, TECHCRUNCH (Jan. 13, 2022, 7:00 AM GMT+1), https://tcrn.ch/337msC5 [https://perma.cc/8ZQU-7ZBQ] [hereinafter Lomas, *In bad news for US cloud services*].

[319] Sam Schechner & Emily Glazer, *Ireland to Order Facebook to Stop Sending User Data to U.S.*, WALL ST. J. (Sept. 9, 2020, 1:19 PM), https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980 [https://perma.cc/59KE-58LW].

[320] *Id.*

> (C) a provider of a remote computing service …,
>
> (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or
>
> (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).[321]

Certain of these categories may be interpreted broadly, but Google and Facebook, for example, would clearly fit within the definition of "electronic communication service provider."[322] A similar analysis should be done for E.O. 12333.[323]

The difficulty also relates to the business model of these companies which depend upon access to personal data, and it is not clear how that could use supplementary measures to limit that access without changing those business models.[324] Facebook obtained a freeze on the preliminary order, which was issued under the 1995 Directive in relation to a case brought by Maximilian Schrems in 2015,[325] and the Irish High Court lifted the freeze in May 2021. The DPC then gave Facebook six weeks to file submissions.[326]

As of April 2022, there was still no final DPC decision on legality of Facebook's personal data transfers to the United States. Furthermore, in its transfer impact assessment, Facebook reportedly offered no significant supplementary measures to ensure data protection in transfers to the United States and claimed justifications for ignoring the *Schrems II* decision.[327] In the assessment, Facebook's lawyers argue that *Schrems II* was about the Privacy Shield Decision, subject to Article 45 of the GDPR, while Facebook transfers are under SCCs pursuant to Article 46, and that the assessment of U.S. law and practice is materially different under the two articles, and thus that the CJEU's legal reasoning should not be relied on for the transfer assessment.[328]

---

[321] 50 U.S.C. § 1881(b)(4) (2018).

[322] *See Airline Commercial Use of EU Personal Data*, *supra* note 25, at 421 (citations omitted).

[323] *Id*. at 422 (citation omitted).

[324] Lomas, *In Bad News for US Cloud Services*, *supra* note 318.

[325] Data Protection Commission, EU-US Data Transfers - Judicial Review Proceedings (Dec. 3, 2020), https://dataprotection.ie/en/news-media/press-releases/eu-us-data-transfers-judicial-review-proceedings [https://perma.cc/7QAX-V67V].

[326] Padraic Halpin, *Irish Data Regulator Resumes Facebook Data Transfer Probe*, REUTERS (May 21, 2021, 9:28 PM GMT+2), https://www.reuters.com/technology/irish-data-regulator-resumes-facebook-data-transfer-probe-2021-05-21/ [https://perma.cc/G9C7-NNF8].

[327] Natasha Lomas, *Facebook's Internal Assessment of EU-US Data Transfers Shows It Has No Legal Leg to Stand on, Says NOYB*, TECHCRUNCH (Dec. 20, 2021, 2:09 PM GMT+1), https://tcrn.ch/3mjY32w [https://perma.cc/FLM3-5GK2].

[328] Vincent Manancourt, *Despite EU Court Rulings, Facebook Says US Is Safe to Receive Europeans' Data*, POLITICO (Dec. 19, 2021 4:48 pm), https://www.politico.eu/article/despite-

This position on the part of Facebook and its lawyers is very questionable, and disclosure of the transfer impact assessment may put pressure on the DPC to act.[329] However, Facebook's stance is consistent with its previous legal strategy, which has been determined by two authors to be at a low level—compliance (stage two) on a scale of legal strategy ranging from the lowest level—avoidance (stage one) to the highest level—transformation (stage five).[330] Furthermore, Facebook has threatened to shut down Facebook and Instagram services in Europe if it cannot process EEA personal data on US-based servers.[331]

In another interesting development, the Irish supervisory authority is currently investigating the transfer of personal data to China by TikTok, to see if such transfers comply with GDPR requirements.[332] If that investigation leads to a sanction, it would be only the second time that transfers to China have been identified as the subject of an EEA supervisory authority action by this study.

This study now turns to a further decision on cross-border data transfers under a different, but parallel regulation to the GDPR.

C. European Data Protection Supervisor—European Parliament

The European Data Protection Supervisor (EDPS) describes itself as "the European Union's (EU) independent data protection authority."[333] The processing of personal data by EU institutions is excluded from the scope of the GDPR, however other legislation covers that case—the European Union Data Protection Regulation (EUDPR).[334] While its decisions may not seem to be directly relevant

---

eu-court-ruling-facebook-says-us-is-safe-to-receive-europeans-data/ [https://perma.cc/R3GY-LY9X].

[329] *Id*. ("… several legal experts contacted by POLITICO said they could not see how Facebook would be able to conclude the U.S. protections are essentially equivalent to the EU's in light of the court ruling. One said that this was especially true for Facebook, since the company's own data transfers were at the heart of the case. The revelations heap fresh pressure on the Irish Data Protection Commission (DPC)…).

[330] *See Personal Data and the GDPR*, *supra* note 21, at 331-33. Voss and Houser apply a legal strategy model created by Robert Bird and then developed by him and David Orozco. *See* Robert C. Bird & David Orozco, *Finding the Right Corporate Legal Strategy*, 56 MIT SLOAN MGT. REV. 81, 82 (2014).

[331] Tim de Chant, *Meta May Be Forced to Shutter Facebook, Instagram in EU*, ARS TECHNICA (Feb. 7, 2022, 6:18 PM), https://arstechnica.com/tech-policy/2022/02/meta-may-be-forced-to-shutter-facebook-instagram-in-eu/ [https://perma.cc/YSP7-G8CX].

[332] Data Protection Commission, DPC launches two inquiries into TikTok concerning compliance with GDPR requirements relating to the processing of childrens' personal data and transfers of data to China, Sept. 14, 2021, https://www.dataprotection.ie/en/news-media/latest-news/dpc-launches-two-inquiries-tiktok-concerning-compliance-gdpr-requirements-relating-processing [https://perma.cc/4FPT-XD9L].

[333] *About Us*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/about/about-us_en [https://perma.cc/ZGQ9-LWGP].

[334] GDPR, *supra* note 5, at art. 2(3) ("For the processing of personal data by the [European] Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other [European] Union legal acts applicable to such processing

to companies involved in cross-border flows of EU personal data, they may provide an interesting view of the thinking of the EDPS, which is influential in data protection, sits on the EDPB,[335] and has voting rights for the EDPB's dispute resolution decisions when they concern principles and rules applicable to EU institutions, bodies, offices and agencies corresponding in substance to those existent under the GDPR.[336]

On January 5, 2022, the EDPS adopted a decision in response to a complaint signed by certain members of the European Parliament involving one of the latter's websites.[337] The Parliament contract with a private company (Ecolog) to conduct mass COVID-19 PCR testing and to run a website allowing online registration for the testing. Complainants learned that the relevant website used Google Analytics.[338] The Parliament admitted the possibility that a transfer of personal data did occur to the United States, in cases "where users connected to the webpage from private connections outside the network of the European Parliament, accepted the cookies from the website and did not have cookies disabled in their browsers."[339] The EDPS considered the Parliament the controller in this case, making it responsible for evaluating the guarantees provided by the processor,[340] and assigning the Parliament the "primary duty of compliance."[341]

The EDPS found that tracking cookies, such as those of Google Analytics, were personal data, and personal data were processed through the trackers. Here the EDPS referred to Google's reply to the DSB in the NetDoktor case discussed in Section A.5 above that "all data collected through Google Analytics is hosted (i.e. stored and further processed) in the USA" for the conclusion that data transfers to the United States took place.[342] The EDPS took the view that, following the *Schrems II* ruling, "transfers of personal data to the US can only take place if they are framed by effective supplementary measures in order to ensure an

---

of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98." Note that Regulation (EC) No 45/2001 has been repealed and replaced by Regulation (EU) 2018/1725 of 23 October 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No 45/2001 and Decision No 1247/20002/EC, 2018 O.J. (L 295) 39 (Nov. 21, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN [https://perma.cc/T2J2-T86E]).

[335] GDPR, *supra* note 5, at art. 68(3).

[336] *Id*. at art. 68(6).

[337] European Data Protection Supervisor, Decision of the European Data Protection Supervisor in Complaint Case 2020-1013 Submitted by Members of the Parliament Against the European Parliament (Jan. 5, 2022), at 1, https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf [https://perma.cc/9TPJ-GACZ].

[338] *Id*. at 2.

[339] *Id*. at 6.

[340] *Id*. at 8.

[341] *Id*. at 9-10.

[342] *Id*. at 13.

essentially equivalent level of protection for the personal data transferred," however the Parliament brought no evidence of such measures to supplement the SCCs on which it relied. Thus, the EDPS found that there had been violations of the provisions on transfers of personal data to third countries or international organizations of the EUDPR.[343]

This case further highlights the need for investigation of personal data flows through a kind of "due diligence," which includes in its scope "any third-party providers, plug-ins or other bits of embedded code," to avoid sanction.[344] In addition, it highlights the point developed in the NetDoktor case, that the use of cookies may involve cross-border data transfers, and these may lead to sanction in the absence of proper supplementary measures. It also presages further decisions of a similar nature in the future.[345]

D. Conclusion on EEA Enforcement Actions

In sum, data exporters must understand their obligations under the GDPR, including security obligations, and ensure that processors have technical and organizational measures in place also to ensure good personal data security. Data transfer tools, when used, must be properly administered, and if a transfer assessment indicates they are required, supplemental measures should be employed.[346] That transfer assessment is akin to due diligence and it must include an evaluation of whether it is possible for the data importer in the destination country to comply with their transfer tool obligations, given the local legislation and practice.[347] Particularly problematic are cases where there is a potential for public authorities to access such data for surveillance purposes in conditions where European fundamental rights and freedoms are respected. Companies need to be aware that the use of tracking cookies and other online services may involve data transfers and should perform a transfer assessment on those transfers, as well as direct transfers.[348] Data transfer requirements apply to any destination third country, which does not benefit from an existing Commission adequacy decision.[349] Finally, companies should monitor the progress of the Facebook case in Ireland for insights that it may bring.

VII. LESSONS FOR COMPLIANCE

First, companies should identify mechanisms on which they base their data transfers. They should no longer be basing transatlantic data transfers on the

---

[343] *See id*. at 14.

[344] Natasha Lomas, *European Parliament Found to Have Broken EU Rules on Data Transfers and Cookie Consents*, TECHCRUNCH (Jan. 11, 2022, 1:00 AM), https://tcrn.ch/3HRKFuS, [https://perma.cc/M2TM-9P2P].

[345] *See* Matt Burgess, *supra* note 125.

[346] *See id*.

[347] *See Recommendations 01/2020 V.2*, *supra* note 214, at 3-4.

[348] *See* Matt Burgess, *supra* note 125 (discussing how cookies were sending information to the US); *see also Recommendations 01/2020 V.2*, supra note 204, at 10-11, 15.

[349] *See Recommendations 01/2020 V.2*, *supra* note 214, at 12-13.

Privacy Shield Decision, which has been invalidated, although they may continue to have liability with respect to their obligations under the Privacy Shield,[350] if they were on the Privacy Shield List. This is true despite the DoC's enigmatic affirmation that it "will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List."[351] If not already accomplished, companies that transfer EEA personal data to the United States, whether directly or indirectly, should choose to replace the Privacy Shield by a data transfer mechanism such as SCCs[352] based on the 2021 SCC Decision.[353] If they need a transfer mechanism for intra-group transfers, BCRs are the evident choice.[354]

Even if the announced Trans-Atlantic Data Privacy Framework is finally agreed upon, this will take time, and today cannot be counted upon. As an example, the procedure for an adequacy decision sketched in Part III.E. took nearly half a year in the case of the Privacy Shield Decision—from February 2, 2016 (when an agreement on first version of the Privacy Shield Agreement was announced, although full documentation came later, on February 29, 2016)[355] until August 1, 2016 (when the final version became applicable).[356] Furthermore, it is questionable whether any replacement framework would be able to survive a new court challenge, which is likely, without a reform of U.S. surveillance laws.[357] It is likely that the new framework, if finally implemented, will be challenged in court, as unnamed officials have been reported to have cautioned.[358] Indeed, an initial reaction from Max Schrems (litigant in *Schrems I* and *Schrems II*), honorary chair of data privacy NGO *noyb*, was that a

---

[350] *Privacy Shield Program Overview*, PRIV. SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview [https://perma.cc/6DDF-LSVB].

[351] *Id.*

[352] *See, e.g.*, Jonathan Kirsop, *Data Transfers Demand Due Diligence After 'Schrems II'*, PINSENT MASONS (Aug. 11, 2020, 10:16 AM), https://www.pinsentmasons.com/out-law/analysis/data-transfers-demand-due-diligence-after-schrems-ii [https://perma.cc/7J53-HUWS].

[353] *See* European Commission Press Release IP/21/2847, European Commission adopts new tools for safe exchanges of personal data (June 4, 2021).

[354] *See Binding Corporate Rules*, PWC, https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf [https://perma.cc/94XA-UTNQ] ("BCRs can be tailored to fit the needs of the business and once implemented and operational, are much easier to maintain compared to intra-group contracts incorporating SCCs.").

[355] *See The Future of Transatlantic Data Flows*, *supra* note 37, at 11-12.

[356] *EU-U.S. Privacy Shield fully operational from today*, EUR. COMM'N (Aug. 1, 2016), https://ec.europa.eu/newsroom/just/items/33704 [https://perma.cc/RY8W-YN4E].

[357] *See, e.g.*, Matt Burgess, *supra* note 125 ("Ultimately the ongoing legal wranglings and political negotiations may open up Privacy Shield's replacement to more legal scrutiny. . .").

[358] Manancourt & Scott, *supra* note 131 ("Other officials cautioned that whatever senior political leaders wanted in terms of securing a new data transfer agreement would sill likely be challenged in Europe's highest court.").

"*Schrems III*" challenge was possible, if the Trans-Atlantic Data Privacy Framework "is not in line with E.U. law."[359]

If the Trans-Atlantic Data Privacy Framework is finally implemented, companies could then use that transfer mechanism, which would likely be subject to periodic review by the Commission. This was the case for its predecessor the Privacy Shield.[360] Given the uncertainty that may be generated by ongoing review and the threat of court challenge, companies may, however, decide that it is more efficient to adapt their internal processes to the SCCs based on the 2021 SCC Decision, instead, thus avoiding any disruption in their transfers in the event that the new framework is invalidated. In any event, these developments need to be monitored on an ongoing basis.

Second, potentially the most important lessons for compliance may be that data exporters must know their transfers—which is to say, map their data flows—and do a focused but "thorough and robust" transfer impact assessment, including justifications for the transfer.[361] This assessment, which has been described as a form of "due diligence," should now, following the NetDoktor decision, cover tracking cookies as well as direct transfers.[362] Companies should also remember that "remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer."[363] Indeed, in order to correctly conduct the assessment, a full understanding of the requirements of *Schrems II* (which include the requirement of respect for the essence of fundamental rights and freedoms, discussed in Part IV.B.3) must be gained. The destination country law and practice, and the transfer tool, taken together, should allow for enforceable data subject rights and effective remedies. As part of the assessment,

---

[359] David McCabe & Matina Stevis-Gridneff, *U.S. and European Leaders Reach Deal on Trans-Atlantic Data Privacy*, N.Y. TIMES (Mar. 25, 2022), https://www.nytimes.com/2022/03/25/business/us-europe-data-privacy.html [https://perma.cc/GKD4-JN2X] ("But it was unclear if the new pact would be enough to satisfy the concerns of privacy campaigners. Max Schrems, an activist whose group Noyb (as in: 'none of your business') has led efforts to invalidate the trans-Atlantic agreements, said in a statement that he was skeptical of the deal and that his organization would carefully analyze the details. 'If it is not in line with E.U. law, we or another group will likely challenge it,' he said."). *See also "Privacy Shield 2.0"? – First Reaction by Max Schrems*, NOYB (Mar. 25, 2022), https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems [https://perma.cc/XG6U-R4VV].

[360] *See, e.g.*, *Cross-Border Data Flows, supra* note 2, at 514 n.167.

[361] *See* Bryant, *supra* note 311 (Companies should "invest into thorough and robust transfer impact assessments. These transfer impact assessments, which should also include a reasoning why a certain data transfer is without alternative, will at least reduce the risk, even if not able to eliminate it in most cases.").

[362] *See*, *e.g.*, Jonathan Kirsop, *Cookies Should Form Part of Data Transfers Due Diligence*, PINSENT MASONS (Jan. 14, 2022, 11:09 AM), https://www.pinsentmasons.com/out-law/news/cookies-should-form-part-of-data-transfers-due-diligence [https://perma.cc/66B5-HMED].

[363] *Recommendations 01/2020 V.2*, *supra* note 214, at 11.

a determination must be made on whether the data importer can comply with its obligations under the chosen transfer mechanism under the laws and practices of the destination country. To help data exporters, the EDPB has set out "Possible Sources of Information to Assess a Third Country," which include European case law, adequacy decisions, transparency reports, and many other ideas about where to start research.[364] If the data importer cannot comply with its obligations, there should be a suspension of transfers and potential a termination of the transfer mechanism contract.

Third, for problematical jurisdictions, such as the United States, something more will likely be required to transfer data lawfully. The transfer impact assessment should determine if this is the case and should identify the proper transfer tool and any appropriate supplementary measures needed, whether they be other contractual ones, technical ones, or organizational ones. Pride of place, with respect to technical measures, goes to strong encryption before transmission of the personal data, reliably managing encryption keys kept under the control of the data exporter, proper use of pseudonymization and split or multi-party processing, depending on the circumstances. In this analysis, consideration should be given as whether the personal data being transferred may be subject to surveillance, either in the hands of the data exporter, the data importer, or in transit. For example, is one of the parties subject to surveillance legislation, such as (in the United States) Section 702 FISA or E.O. 12333? If a U.S. Big Tech cloud computing provider is in the loop, for example, then surveillance legislation likely applies.[365]

Fourth, as was seen in the NetDoktor case, the use of tracking cookies may involve inadvertent transfers of European personal data to third country such as the United States.[366] Companies should consider limiting the number of cookies used on their websites. This is consistent with the concept of data minimization, which is enshrined as a data quality principle among the data protection principles in the GDPR: "Personal data shall be: … (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."[367] One example of how data minimization may be applied by a data exporter is provided by the EDPB: "identify those sets of data that are not necessary for the purposes of the transfer and, therefore, won't be shared with the data importer.[368] European alternatives to service providers may also be considered in connection with services provided by those whose cookies are placed on websites, thereby avoiding a transfer outside of the EEA.

Fifth, there may be a definite advantage gained through use of cloud and other service providers located within the EEA and use of contracts providing clearly

---

[364] *Id*. annex 3 at 47-48 (providing a list of categories of sources and a few weblinks).

[365] *See, e.g.*, *Airline Commercial Use of EU Personal Data*, *supra* note 25, at 421-22 (citations omitted).

[366] *See* Matt Burgess, *supra* note 125.

[367] GDPR, *supra* note 5, at art. 5(1)(c).

[368] *Recommendations 01/2020 V.2*, *supra* note 214, annex 2, at 45.

that there will be no data processing in third countries. Reportedly, this has pushed tech giants such as Google, Microsoft and and TikTok to store more data in Europe.[369] This effect may be referred to as "soft" data localization,[370] which is a contrast with "hard" data localization laws in China and Russia,[371] for example, as it is not forced but chosen data localization, even if there might be a friendly nudge to do so. However, this suggestion will displease trade liberalists.

CONCLUSION

The use of data plays an important role in today's economy and hard data localization and data transfer restrictions provide challenges for trade. The GDPR sets out requirements for cross-border personal data transfers outside of the EEA. Unless a third country benefits from a Commission adequacy decision, attesting to its adequate data protection, personal data may not be transferred there from the EEA without something more—a transfer tool, such as the popular SCCs or BCRs. However, companies should perform a transfer impact assessment prior to engaging in transfers. That exercise, which is a form of due diligence, must involve an evaluation of the respect of the essence of fundamental rights in the destination country, taking into consideration the transfer tool.

In 2016, the United States benefited from a treatment of favor—recognizing the importance of the Europe-U.S. trade relationship—when the Privacy Shield Decision was adopted, allowing U.S. companies to self-certify to compliance with the Privacy Shield Principles and transfer personal data from the EEA to the United States. This was so even though the United States still does not have an omnibus federal data privacy law that could be considered as adequate data protection, from a European perspective. In a CJEU case involving Facebook and aimed at SCCs, the CJEU found that, in using the Privacy Shield the essence of fundamental rights in the United States was not respected, and that something more was needed. Consequently, the EDPB proposed supplemental measures that companies may use to ensure GDPR compliance, which are detailed in this study.

This study has also surveyed EEA enforcement action, and through an analysis of these decisions and EDPB guidance, has distilled lessons for compliance for companies. Good personal data transfer tool administration and proper use of encryption are well placed on this list. One controversial suggestion, that may result from the NetDoktor case, involves the use of what may be described as soft data localization. Companies cannot today count on a quick replacement for the Privacy Shield, considering the apparent American

---

[369] *See* Manancourt & Kayali, *supra* note 312.

[370] Chander defines this term as, "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." Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771, 772 (2020).

[371] *See Cross-Border Data Flows, supra* note 2, at 501-02.

distaste for modifying their relevant surveillance law, which makes a quick fix unlikely and perhaps localization of data in the EEA more palatable.

Finally, this study has shown that the concerns now addressed with respect to the United States following the *Schrems II* ruling, are also relevant to other jurisdictions. Even more reason to monitor developments, such as those of the case of Facebook's data transfers before the Irish supervisory authority, given the importance of personal data in the context of today's global economy. Furthermore, it is also an incentive to understand the parameters of EEA legal requirements analyzed in this study, given the importance of the European bloc in international trade and the potentially high fines that may be imposed under the GDPR.