# PRIVACY SHIELD 2.0— A NEW TRANS-ATLANTIC DATA PRIVACY FRAMEWORK BETWEEN THE EUROPEAN UNION AND THE UNITED STATES

*Sara Gerke*† *and Delaram Rezaeikhonakdar*††

*This Article is the first to thoroughly examine the new adequacy decision for the Trans-Atlantic Data Privacy Framework (also known as "Privacy Shield 2.0"), including the relevant events and milestones ultimately leading to its adoption. The European Commission adopted the new Privacy Shield on July 10, 2023, to restore transatlantic data flows and commercial exchanges between the European Union and the United States. This Article first explores the holdings of the Court of Justice of the European Union in the groundbreaking cases* Schrems I *and* Schrems II *and elaborates on the reasons for the invalidation of the Safe Harbor Decision and the Privacy Shield Decision, respectively. It then examines the practical implications of the invalidation of the Privacy Shield Decision in Schrems II, including the recent decision of the Irish Data Protection Commissioner regarding Meta Platforms*

† Assistant Professor of Law, Penn State Dickinson Law, Carlisle, PA, USA; Co-Principal Investigator, WP8 (Legal, Ethical & Liability), Validating AI in Classifying Cancer in Real-Time Surgery (CLASSICA), European Union (Grant Agreement no. 101057321); Co-Principal Investigator, WP4 (Addressing Ethical/Legal Concerns), Optimizing Colorectal Cancer Prevention through Personalized Treatment with Artificial Intelligence (OperA), European Union (Grant Agreement no. 101057099); Multiple Principal Investigator, Bioethical, Legal, and Anthropological Study of Technologies (BLAST), National Institute of Biomedical Imaging and Bioengineering (NIBIB) and the National Institutes of Health Office of the Director (NIH OD) (Grant Agreement no. 1R21EB035474-01); Co-Investigator (Supplemental Project), PREMIERE: A PREdictive Model Index and Exchange Repository, NIBIB and NIH OD (Grant Agreement no. 3R01EB027650-03S1); Co-Investigator, Penn State TCORS: Tobacco Product Composition Effects on Toxicity and Addiction, National Institute on Drug Abuse (NIDA)/National Institutes of Health (NIH) (Grant Agreement no. 1U54DA058271-01). This Article greatly benefited from feedback from participants at the 2023 Health Law Professors Conference organized by the American Society of Law, Medicine & Ethics and the University of Maryland Francis King Carey School of Law. We thank Kaci McNeave and Robin Platte for their assistance with footnote formatting. All errors are our own. Correspondence to sgerke@psu.edu.

†† S.J.D. Candidate, Penn State Dickinson Law, Carlisle, PA, USA.

*Ireland Limited (formerly Facebook Ireland Limited). This Article subsequently discusses the efforts of the United States government and the European Commission toward the adoption of Privacy Shield 2.0. It analyzes recent events, from the announcement of a new Trans-Atlantic Data Privacy Framework to the release of the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities to the European Commission's draft adequacy decision, the launch of its adoption process, and ultimately its adoption.*

*This Article argues that despite the excitement of a new Trans-Atlantic Data Privacy Framework, it is improbable that the validity of Privacy Shield 2.0 would be upheld by the Court of Justice of the European Union in a possible Schrems III case. Although Privacy Shield 2.0 is a considerable improvement compared to the previously invalidated Privacy Shield Decision, it is likely that the Court of Justice of the European Union would consider the newly introduced safeguards for United States signals intelligence activities insufficient to comply with the General Data Protection Regulation's requirements, read in the light of the Charter of Fundamental Rights of the European Union. This Article demonstrates the shortcomings of Privacy Shield 2.0 concerning the principles of necessity and proportionality as well as the right to effective judicial protection. It also argues for a comprehensive U.S. federal privacy law that ensures adequate protection of personal data for all data subjects in the United States.*

## TABLE OF CONTENTS

## INTRODUCTION

The cross-border transfer of personal data from the European Union to the United States has a significant impact on EU-U.S. trade and investment relations in addition to strengthening the capacity of companies in terms of "online communication, track[ing] global supply chains, shar[ing] research, provid[ing] cross-border services, and support[ing] technological innovation, among other activities."[1] In 2020 alone, the EU-U.S. trade of information and communications technology(-enabled) services amounted to more than $264 billion, reflecting the importance of an enduring positive relationship across the Atlantic.[2]

The General Data Protection Regulation (GDPR)[3] has been applied in the EU Member States since May 25, 2018, to the processing of personal data.[4] Personal data is "any information relating to an identified or identifiable natural person ('data subject')."[5] The GDPR not only applies to EU-established controllers or processors but also to those *not*

1 RACHEL F. FEFER & KRISTIN ARCHICK, CONG. RSCH. SERV., IF11613, U.S.-EU TRANS-ATLANTIC DATA PRIVACY FRAMEWORK 1 (2022), https://crsreports.congress.gov/product/pdf/IF/IF11613 [https://web.archive.org/web/20230602173309/https://crsreports.congress.gov/product/pdf/IF/IF11613].

2 *Id.*

3 Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

4 *Id.* arts. 2, 99(2).

5 *Id.* art. 4(1).

established in the EU, such as those established in the United States "where the processing activities are related to . . . the offering of goods or services" to EU data subjects or "the monitoring of their behaviour as far as their behaviour takes place within the Union."[6] A "controller" is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[7] A "processor" on the other hand is "a natural or legal person, public authority, agency or other body which processes personal data *on behalf of the controller*."[8]

The GDPR also applies when personal data is transferred from the EU to a third country, such as the United States.[9] As a general principle, cross-border transfer of personal data from the EU to a third country is prohibited unless the transfer is based on one of the mechanisms introduced in Chapter V of the GDPR.[10] One of these mechanisms, which is the focus of this Article, is the European Commission's (EC) adoption of a so-called "adequacy decision" under Article 45(3) of the GDPR. The EC assesses a third country's "adequacy of the level of protection" and "decide[s], by means of implementing act," whether that country "ensures an adequate level of protection."[11] If so, the GDPR allows the transfer of personal data from the EU to that country without the requirement of "any specific authorisation."[12] In its assessment of a third country, the EC needs to take into consideration different elements, ranging from "the rule of law" and "respect for human rights and fundamental freedoms" to general and sectoral legislation, "including concerning public security, defence, national security and criminal law and the access of public authorities to personal data."[13] A third country ensures "an adequate level of protection" if it has an "essentially

6 *Id.* art. 3(1)–(2).

7 *Id.* art. 4(7).

8 *Id.* art. 4(8) (emphasis added).

9 *Id.* art. 44. For the GDPR to apply to such personal data transfers, only the exporter (i.e., the EU-established controller or processor) must be subject to Article 3 of the GDPR; it is not necessary that the importer (i.e., the controller or processor in the third country) also be subject to Article 3 of the GDPR concerning the given processing activity. For more information, see generally Eur. Data Prot. Bd., *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* (Feb. 14, 2023), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en [https://perma.cc/R6P6-NKAJ].

10 GDPR, *supra* note 3, art. 44.

11 *Id.* art. 45(1)–(3).

12 *Id.* recital 103, art. 45(1).

13 *Id.* recital 104, art. 45(2)(a).

equivalent"—not necessarily identical—level of data protection to what is guaranteed in the EU.[14]

Without an adequacy decision, Article 46 of the GDPR only allows transfers of personal data from the EU to a third country "subject to appropriate safeguards."[15] An example of an alternative mechanism for cross-border transfers is the so-called "standard contractual clauses" (SCCs).

The EC has so far adopted adequacy decisions for the following 15 countries: "Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED [Law Enforcement Directive], the United States (commercial organisations participating in the EU-U.S. Data Privacy Framework) and Uruguay."[16]

Most recently, on July 10, 2023, the EC adopted a new adequacy decision for the Trans-Atlantic Data Privacy Framework (Privacy Shield 2.0).[17] Privacy Shield 2.0, which this Article focuses on, came into force on the date of its adoption and helps restore transatlantic data flows by allowing entities in the European Economic Area (EEA) to transfer personal data to certified U.S. companies without the need for "additional data protection safeguards."[18]

As mentioned, the EC's adoption of an adequacy decision under Article 45(3) of the GDPR precedes an assessment of the third country's

---

14 *Id.* recital 104, art. 45(1). The EU Data Protection Authorities published guidance to the European Commission and the WP29 under the GDPR for the assessment of the level of data protection in third countries and international organizations by establishing the core data protection principles that have to be present in a third country legal framework or an international organization in order to ensure essential equivalence with the EU framework. *See* Art. 29 Data Prot. Working Party, *Adequacy Referential*, at 2, WP 254 rev.01 (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/redirection/document/57550 [https://perma.cc/EN3W-JSJM].

15 GDPR, *supra* note 3, art. 46.

16 *Adequacy Decisions: How the EU Determines If a Non-EU Country Has an Adequate Level of Data Protection*, EUROPEAN COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/UBX7-FFRV].

17 Commission Implementing Decision 2023/1795, 2023 O.J. (L 231) 118 (EU) [hereinafter Adequacy Decision—Privacy Shield 2.0].

18 European Commission Press Release IP/23/3721, Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows (July 10, 2023), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_3721/IP_23_3721_EN.pdf [https://perma.cc/A7DF-H44D]; European Commission Questions & Answers QANDA/23/3752, EU-US Data Privacy Framework (July 10, 2023), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_23_3752/QANDA_23_3752_EN.pdf [https://perma.cc/49P3-FB7X]. The EEA includes the 27 EU Member States, Iceland, Liechtenstein, and Norway. *Id.*

"adequacy of the level of protection."[19] To decide whether this is the case, the relevant case law must also be taken into account.[20] Since 2013, the concern of an Austrian resident, Maximilian Schrems, about the failure of the United States to recognize the privacy rights of EU data subjects has led to two groundbreaking cases before the Court of Justice of the European Union (CJEU), namely *Maximilian Schrems v. Data Protection Commissioner* (*Schrems I*)[21] and *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems* (*Schrems II*).[22] In both *Schrems I* and *Schrems II*, the CJEU declared the EC's respective decisions on whether the United States "ensures an adequate level of protection" to be invalid. *Schrems I* invalidated Decision 2000/520 (Safe Harbor Decision),[23] which was adopted on the basis of Article 25(6) of Directive 95/46/EC[24] (the previous Directive repealed by the GDPR) and allowed transfers of personal data from the EU to the United States. *Schrems II* subsequently invalidated Decision 2016/1250 (Privacy Shield Decision),[25] which served as the invalidated Safe Harbor Decision's replacement.

During the nearly three years between the invalidation of the Privacy Shield Decision in *Schrems II* and the adoption of a new adequacy decision, companies and others faced significant uncertainties and hurdles in lawfully transferring personal data from the EU to the United States. Without an adequacy decision, they had no choice but to stop cross-border transfers of personal data altogether or use one of the other available but more time-consuming and costly mechanisms, such as SCCs. An adequacy decision has a huge advantage in that transfers of personal data from the EU to the United States can take place without the need for additional safeguards or authorizations.[26] To restore transatlantic data flows and commercial exchanges between the EU and

---

19 GDPR, *supra* note 3, art. 45(2).

20 Adequacy Decision—Privacy Shield 2.0, *supra* note 17 recital 3.

21 Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015).

22 Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020).

23 Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC) [hereinafter Decision 2000/520—Safe Harbor Decision].

24 Directive 95/46, 1995 O.J. (L 281) 31 (EC).

25 Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1 (EU) [hereinafter Decision 2016/1250—Privacy Shield Decision].

26 GDPR, *supra* note 3, recital 103, art. 45(1); European Commission Factsheet MEMO/17/15, Digital Single Market—Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers (Jan. 10, 2017), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_17_15/MEMO_17_15_EN.pdf [https://perma.cc/6HWT-R283].

the United States, it is thus not surprising that the U.S. government and the EC made significant efforts toward the adoption of a new Privacy Shield.

This Article is the first to thoroughly analyze the new adequacy decision for the Trans-Atlantic Data Privacy Framework, including the relevant events and milestones ultimately leading to its adoption. First of all, it should be noted that Privacy Shield 2.0 has been the focus of intense political debate. The United States and the EU have their own legitimate reasons for their actions; this Article does not represent one side or the other, but rather seeks to objectively analyze and answer the following legal question: Can the Privacy Shield 2.0 stand its ground before the CJEU in a possible *Schrems III* case? Or, in other words: Would the CJEU likely uphold the validity of the Privacy Shield 2.0 on the grounds that the United States ensures an adequate level of protection under Article 45 of the GDPR, read in light of the Charter of Fundamental Rights of the EU (Charter),[27] or rather invalidate Privacy Shield 2.0 like its predecessors?

This Article consists of four Parts. Part I discusses the CJEU's holdings in *Schrems I* and *Schrems II* and maps out the court's rationale for invalidating the Safe Harbor Decision and the Privacy Shield Decision, respectively. It compares both cases and draws lessons learned to understand better what changes to U.S. laws and practices are needed for a new Privacy Shield to be able to stand its ground before the CJEU in a possible *Schrems III* case. In particular, Part I shows that neither the Safe Harbor Decision nor the Privacy Shield Decision limited interference with fundamental rights to what is strictly necessary. Both adequacy decisions also did *not* provide data subjects with the right to effective judicial protection.

Part II explores the practical implications of the invalidation of the Privacy Shield Decision in *Schrems II.* It discusses the challenges companies and others faced in the past almost three years when using alternative mechanisms, especially SCCs, for cross-border transfers of personal data from the EU to the United States. In particular, Part II shows that, although the CJEU upheld the validity of Decision 2010/87 (SCC Decision)[28] in *Schrems II*, the court highlighted the need for "supplementary measures" to compensate for any lack of data protection.[29] However, the CJEU did not further specify what such measures could look like, which has led to significant uncertainty among companies and others about lawfully using SCCs to transfer personal data

---

27 Charter of Fundamental Rights of the European Union, arts. 7, 8, 47, 2000 O.J. (C 364) 1 [hereinafter Charter].

28 Commission Decision 2010/87, 2010 O.J. (L 39) 5 (EU) [hereinafter Decision 2010/87—SCC Decision].

29 Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 133 (July 16, 2020).

from the EU to third countries. To highlight these challenges, Part II also discusses the recent decision of the Irish Data Protection Commissioner (DPC) from May 2023 concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited).

Part III explores the U.S. government's and the EC's efforts toward the adoption of Privacy Shield 2.0, beginning with the March 2021 announcement of a new Trans-Atlantic Data Privacy Framework between the EU and the United States, followed by the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities of October 7, 2022 (EO 14086),[30] and concluding with the EC's draft adequacy decision of December 13, 2022,[31] the launch of its adoption process, and ultimately its adoption. In particular, Part III thoroughly examines the new safeguards for U.S. signals intelligence activities and the two-layer redress mechanism introduced by sections 2 and 3 of EO 14086. It is particularly important to understand these changes in order to assess whether the CJEU's concerns in *Schrems I* and *Schrems II* have been properly addressed.

Part IV analyzes EO 14086 to assess whether and to what extent the new safeguards might meet the CJEU scrutiny in *Schrems I* and *Schrems II*. It argues that although Privacy Shield 2.0 is certainly an improvement to the previously invalidated Privacy Shield Decision, it is improbable that the CJEU would uphold its validity in a possible *Schrems III* case. The CJEU would likely strike Privacy Shield 2.0 down on the grounds that the United States fails to ensure an adequate level of protection under Article 45 of the GDPR, read in light of Articles 7, 8, and 47 of the Charter. In particular, Privacy Shield 2.0 could be more robust with regard to the satisfaction of the principles of necessity and proportionality and the right to effective judicial protection.

Consequently, this Article argues that the EC should have refrained from adopting Privacy Shield 2.0 and instead continued negotiations with the United States to address the identified weaknesses. In the interest of companies and data subjects in particular, Privacy Shield 2.0 should only have been adopted if it had been robust enough to likely stand its ground before the CJEU. In addition, the United States urgently needs a comprehensive privacy law at the federal level to ensure adequate protection of personal data for all data subjects in the United States. Such

---

30 Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 7, 2022).

31 Commission Implementing Decision of XXX Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework (Dec. 13, 2022), https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf [https://perma.cc/UMZ3-A4W7] [hereinafter Draft Adequacy Decision].

a law could ultimately also help demonstrate an essentially equivalent level of data protection to what is guaranteed in the EU.

## I. *SCHREMS I*, *SCHREMS II*, AND KEY TAKEAWAYS

This Part first discusses the relevant events that led to *Schrems I* and *Schrems II*, including the main reasons why the CJEU invalidated the Safe Harbor Decision and the Privacy Shield Decision, respectively. It then compares both groundbreaking cases and draws lessons from them.

### A. *Schrems I*

In June 2013, Maximilian Schrems, a Facebook user and a resident of Austria, filed a formal complaint with the Irish DPC against Facebook Ireland Limited.[32] In his complaint, Schrems challenged the transfer of his personal data from Facebook Ireland Limited to Facebook, Inc. in the United States.[33] His concern was in light of the leaking of U.S. National Security Agency (NSA) documents by Edward Snowden, a former NSA computer intelligence contractor.[34] Schrems complained to the DPC that Facebook, Inc. granted "'mass access'" to "user data to the NSA for reasons of espionage, national security and other matters . . . without any need for a probable cause since June 3rd 2009 under a program called 'PRISM.'"[35]

The DPC refused to investigate Schrems's complaint, calling it "frivolous and vexatious" because Facebook, Inc. had self-certified under the EC's Safe Harbor Decision.[36] On July 26, 2000, the EC adopted the Safe Harbor Decision in accordance with Article 25(6) of Directive 95/46/EC, recognizing that the United States ensured "an adequate level

32 Complaint Against Facebook Ireland Ltd from Maximilian Schrems, to Data Prot. Comm'r 1 (June 25, 2013) [hereinafter 2013 Complaint Against Facebook Ireland Ltd], https://noyb.eu/sites/default/files/2020-07/complaint-PRISM-facebook_2013.pdf [https://perma.cc/SVT4-8AB3].

33 *Id.*

34 Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013, 3:23 PM), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/4G68-PDPT]; Nicholas Watt, *Prism Scandal: European Commission to Seek Privacy Guarantees from US*, THE GUARDIAN (June 10, 2013, 9:52 AM), https://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees [https://perma.cc/PB4U-F5X6].

35 2013 Complaint Against Facebook Ireland Ltd, *supra* note 32, at 1.

36 Schrems v. Data Prot. Comm'r [2014] IEHC 310, ¶ 32 (H. Ct.) (Ir.).

of protection."[37] The Safe Harbor Decision allowed the transfer of personal data from the EU to the United States "without additional guarantees being necessary."[38]

Schrems subsequently brought an action before the High Court of Ireland for a judicial review.[39] The High Court decided to refer questions relating to the validity of the Safe Harbor Decision to the CJEU for a preliminary ruling.[40]

In *Schrems I*, the CJEU investigated whether the Safe Harbor Decision was a valid basis for the cross-border transfer of personal data from the EU to the United States.[41] On October 6, 2015, the CJEU invalidated Decision 2000/520 (i.e., the Safe Harbor Decision),[42] relying on several reasons for so doing.

The CJEU first observed that the Safe Harbor Principles, as set out in Annex I to Decision 2000/520, implemented in accordance with the frequently asked questions as set out in Annex II, are "applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them."[43] Moreover, the court found:

> Decision 2000/520 lays down that *'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles*, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.[44]

---

37 Directive 95/46, *supra* note 24, art. 25(6). *See also* Decision 2000/520—Safe Harbor Decision, *supra* note 23, recital 5 (delineating "[t]he adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision").

38 Decision 2000/520—Safe Harbor Decision, *supra* note 23, recital 2.

39 Schrems v. Data Prot. Comm'r [2014] IEHC 310 (H. Ct.) (Ir.).

40 *Id.* ¶¶ 71, 84; Consolidated Version of the Treaty on the Functioning of the European Union art. 267, Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter TFEU].

41 *Schrems I*, ECLI:EU:C:2015:650, ¶ 67.

42 *Id.* ¶ 106.

43 *Id.* ¶ 82; *see also* Decision 2000/520—Safe Harbor Decision, *supra* note 23, annex I ("They [the Safe Harbor Principles] are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of 'adequacy' it creates.").

44 *Schrems I*, ECLI:EU:C:2015:650, ¶ 86 (emphasis added); *see* Decision 2000/520—Safe Harbor Decision, *supra* note 23, annex I, ¶ 4 ("Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization . . . ."); *see also id.* annex IV, pt.

The CJEU then clarified that its analysis of the Safe Harbor Decision was based on two 2013 EC Communications,[45] in which

> the Commission found that the *United States authorities were able to access the personal data* transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, *beyond what was strictly necessary and proportionate to the protection of national security.* Also, the Commission noted that the *data subjects had no administrative or judicial means of redress enabling*, in particular, *the data relating to them to be accessed and, as the case may be, rectified or erased.*[46]

The court further stated that "protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is *strictly necessary.*"[47] Consequently, the court observed: "In particular, legislation permitting the public authorities to have *access on a generalised basis* to the content of electronic communications must be regarded as *compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.*"[48]

Moreover, the CJEU found:

> [L]egislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, *does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.*[49]

Furthermore, the CJEU noted:

> [U]nder Article 28 of Directive 95/46, read in the light in particular of Article 8 of the Charter [the right to protection of personal data], the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a

B ("Clearly, where U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law.").

45 *Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows*, COM (2013) 846 final (Nov. 27, 2013); *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).

46 *Schrems I*, ECLI:EU:C:2015:650, ¶ 90 (emphasis added).

47 *Id.* ¶ 92 (emphasis added).

48 *Id.* ¶ 94 (emphasis added).

49 *Id.* ¶ 95 (emphasis added).

> person's rights and freedoms in regard to the processing of personal data relating to him.[50]

However, the court observed that "[t]he first subparagraph of Article 3(1) of Decision 2000/520 . . . den[ies] the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46."[51] Consequently, the CJEU held that "the Commission exceeded the power which is conferred upon it in Article 25(6) of Directive 95/46."[52]

### B. *Schrems II*

Following *Schrems I*, the referring High Court of Ireland annulled the DPC's rejection of Schrems's complaint and referred its decision back to the DPC for investigation.[53] The DPC asked Schrems to restructure his complaint in light of *Schrems I* and Facebook Ireland Limited's explanation that, in large part, personal data was transferred from Facebook Ireland Limited to Facebook, Inc. in the United States in accordance with Decision 2010/87[54]—i.e., an alternative basis for the transfer of personal data from the EU to the United States in the absence of an adequacy decision.[55] Schrems's updated complaint from December 1, 2015, asked the DPC for the prohibition or suspension of transferring his personal data from Facebook Ireland Limited to Facebook, Inc.[56] In particular, Schrems claimed that:

> "Facebook Inc" is subject to a number of known and secret laws, rules, court decisions and executive orders that oblige it to make my personal data available and/or oblige it to disclose it to US authorities, such as e.g. the National Security Agency (NSA) and the Federal Bureau of Investigations (FBI).[57]

Consequently, Schrems concluded that the SCC Decision could not justify the personal data transfer from the EU to the United States.[58]

---

50 *Id.* ¶ 99.

51 *Id.* ¶ 102.

52 *Id.* ¶ 104.

53 Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 54 (July 16, 2020).

54 Decision 2010/87—SCC Decision, *supra* note 28.

55 *Schrems II*, ECLI:EU:C:2020:559, ¶ 54. For more information on SCCs, see *infra* Part II.

56 Complaint Against Facebook Ireland Ltd from Maximilian Schrems, to Data Prot. Comm'r 15 (Dec. 1, 2015) [hereinafter 2015 Complaint Against Facebook Ireland Ltd], https://noyb.eu/sites/default/files/2020-07/comp_fb_ie.pdf [https://perma.cc/LV42-TYME]; *Schrems II*, ECLI:EU:C:2020:559, ¶ 55.

57 2015 Complaint Against Facebook Ireland Ltd, *supra* note 56, at 2.

58 *Id.* at 11; *Schrems II*, ECLI:EU:C:2020:559, ¶ 55.

According to his complaint, through the U.S. mass surveillance programs, "the 'essence' of the fundamental rights of about a billion data subjects under Art 7 [right to respect for private life], 8 [right to protection of personal data] and 47 [right to effective judicial protection] CFR [Charter] are continuously breached."[59]

On May 24, 2016, the DPC issued a draft decision under section 10(1)(b)(ii) of the 1988 and 2003 Data Protection Acts, sharing Schrems's viewpoint on a provisional basis.[60] Shortly after that, on May 31, 2016, the DPC brought an action before the High Court of Ireland, and the High Court, in turn, on April 12, 2018, referred eleven questions to the CJEU for a preliminary ruling.[61]

In *Schrems II*, the CJEU addressed, in particular, whether the Privacy Shield Decision and SCCs were valid mechanisms for cross-border transfers of personal data from the EU to the United States.[62] The EC's Privacy Shield Decision, which replaced the invalidated Safe Harbor Decision, became relevant to this case as it was adopted on July 12, 2016, according to Article 25(6) of Directive 95/46/EC, finding that "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."[63] In addition, the GDPR is relevant to this case because it repealed Directive 95/46/EC with effect from May 25, 2018.[64]

On July 16, 2020, the CJEU invalidated the Privacy Shield Decision.[65] The validity of the SCC Decision, however, was upheld.[66] The court relied on several reasons to invalidate the Privacy Shield Decision.

The CJEU first referred to paragraph I.5. of Annex II of the Privacy Shield Decision, which stated, among other things, "that adherence to those principles [the Privacy Shield Principles, including the

---

59 2015 Complaint Against Facebook Ireland Ltd, *supra* note 56, at 11, 15.

60 Draft Decision of the Data Protection Commissioner under Section 10(1)(b)(ii) of the Data Protection Acts, 1988 & 2003, 3/15/766, 2 (Ir. Data Prot. Comm'n May 24, 2016), https://epic.org/wp-content/uploads/privacy/intl/schrems/20160524-DPC-Draft-Decision.pdf [https://perma.cc/W7H2-S6WR] ("While my investigation remains ongoing, I have formed the view, on a draft basis, and pending receipt of such further submissions as the Complainant and/or FB-I may wish to submit, that a legal remedy compatible with Article 47 of the Charter of Fundamental Rights of the European Union ('the Charter') is not available in the US to EU citizens whose data is transferred to the US where it may be at risk of being accessed and processed by US State agencies for national security purposes in a manner incompatible with Articles 7 and 8 of the Charter.").

61 *Schrems II*, ECLI:EU:C:2020:559, ¶ 57; Request for a Preliminary Ruling Article 267 TFEU at 20–24, Data Prot. Comm'r v. Facebook Ire. Ltd. [2016] No. 4809 P. (H. Ct.) (Ir.).

62 *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 122–202.

63 Decision 2016/1250—Privacy Shield Decision, *supra* note 25, art. 1(1).

64 GDPR, *supra* note 3, art. 94(1).

65 *Schrems II*, ECLI:EU:C:2020:559, ¶ 201.

66 *Id.* ¶ 149. For more information on SCCs, see *infra* Part II.

Supplemental Principles, issued by the Department of Commerce] may be limited . . . 'to the extent necessary to meet national security, public interest, or law enforcement requirements.'"[67] Consequently, the court observed that the Privacy Shield Decision, similar to the Safe Harbor Decision, grants primacy to national security, public interest, and law enforcement requirements, and that, pursuant to this primacy, "self-certified United States organisations receiving personal data from the European Union are bound to disregard the principles [the Privacy Shield Principles, including the Supplemental Principles, issued by the Department of Commerce] without limitation where they conflict with the requirements and therefore prove incompatible with them."[68] Thus, the court found that the Privacy Shield Decision "enables interference . . . with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States."[69] The court mentioned as a potential example of such interference "the PRISM and UPSTREAM surveillance programmes under Section 702 of the [Foreign Intelligence Surveillance Act of 1978] FISA and [Executive Order] E.O. 12333."[70]

The CJEU then analyzed "whether US law in fact ensures the adequate level of protection required under Article 45 of the GDPR, read in the light of the fundamental rights guaranteed in Articles 7, 8 and 47 of the Charter."[71] To begin with, the court clarified that "Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society."[72] In particular, the court stated:

> [I]n accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the *essence of those rights and freedoms*. Under the second sentence of Article 52(1) of the Charter, subject to the *principle of proportionality*, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[73]

The court also clarified that:

---

67 *Schrems II*, ECLI:EU:C:2020:559, ¶ 164 (quoting Decision 2016/1250—Privacy Shield Decision, *supra* note 25, annex II, ¶ I.5).

68 *Id.*

69 *Id.* ¶ 165.

70 *Id.*; Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 8, 1981).

71 *Schrems II*, ECLI:EU:C:2020:559, ¶ 168.

72 *Id.* ¶ 172.

73 *Id.* ¶ 174 (emphasis added).

> [*I*]*n order to satisfy the requirement of proportionality* according to which derogations from and limitations on the protection of personal data must apply only in so far as is *strictly necessary*, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse.[74]

However, the CJEU found "that neither Section 702 of the FISA, nor E.O. 12333 . . . correlates to the minimum safeguards resulting . . . from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions *cannot be regarded as limited to what is strictly necessary*."[75] For example, the court showed "that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes."[76]

In addition, the CJEU held that "the ombudsperson mechanism to which the Privacy Shield Decision refers [in Annex III] 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."[77]

The court clarified that:

> Article 47 requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the *right to an effective remedy before a tribunal* in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled *to a hearing by an independent and impartial tribunal*.[78]

The CJEU noted that "as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333 . . . data subjects have no right to an effective remedy."[79] However, according to the court, the Privacy Shield Decision's introduction of an ombudsperson mechanism[80] could not remedy those deficiencies because the "[o]mbudsperson is appointed by [and directly reports to] the Secretary of State and is an integral part of the US State Department," which would

---

74 *Id.* ¶ 176 (emphasis added).

75 *Id.* ¶ 184 (emphasis added).

76 *Id.* ¶ 180.

77 *Id.* ¶ 197.

78 *Id.* ¶ 186 (emphasis added).

79 *Id.* ¶ 192.

80 *See* Decision 2016/1250—Privacy Shield Decision, *supra* note 25, annex III.

"undermine the [o]mbudsman's independence from the executive."[81] The ombudsperson also lacks "the power to adopt decisions that are binding on those intelligence services."[82]

In summary, the CJEU held that "the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid."[83]

### C. *Comparison and Lessons Learned*

Interferences for national security purposes with the fundamental rights of individuals whose personal data is transferred from the EU to the United States gave rise to *Schrems I* and *Schrems II*. Table 1 below compares the main reasons why the CJEU invalidated the Safe Harbor Decision and the Privacy Shield Decision and illustrates the lessons learned from both cases. This knowledge is particularly relevant to better understand what changes to U.S. laws and practices are needed so that a new Privacy Shield could stand its ground before the CJEU.

| Issue | *Schrems I* | *Schrems II* | Lessons Learned |
|---|---|---|---|
| No satisfaction of the proportionality requirement / no limitation to what is strictly necessary[84] | "[T]he Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, | "It follows therefore that neither Section 702 of the FISA, nor E.O. 12333 . . . correlates to the minimum safeguards resulting . . . from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as | Both the Safe Harbor Decision and the Privacy Shield Decision did not limit interference with fundamental rights to what is "strictly necessary." |

81 *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 190, 195.

82 *Id.* ¶ 196.

83 *Id.* ¶ 199; *see id.* at ¶¶ 200–01.

84 *See* Charter, *supra* note 27, art. 52(1).

| | | | |
|---|---|---|---|
| | beyond what was strictly necessary and proportionate to the protection of national security."[85]<br><br>"In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."[86] | limited to what is strictly necessary."[87] | |
| No legal remedies | "Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or | "Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers [in Annex III] does not provide any cause of action before a body which offers the persons whose data is transferred to the United | Both the Safe Harbor Decision and the Privacy Shield Decision did not provide data subjects with the right to effective judicial protection. |

85 *Schrems I*, ECLI:EU:C:2015:650, ¶ 90.

86 *Id.* ¶ 94.

87 *Schrems II*, ECLI:EU:C:2020:559, ¶ 184.

| | | | |
|---|---|---|---|
| | erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."[88] | States guarantees essentially equivalent to those required by Article 47 of the Charter."[89] | |

*Table 1: Main Reasons Why the CJEU Invalidated the Safe Harbor Decision and the Privacy Shield Decision*

*Schrems II* considerably echoes *Schrems I* in the structure and content of its argumentation. Column 1 in Table 1 demonstrates two common issues in *Schrems I* and *Schrems II*. Columns 2 and 3 explain the reasoning of the CJEU in *Schrems I* and *Schrems II*, respectively, in connection with these issues. Column 4 draws the lessons learned from both cases.

## II. PRACTICAL IMPLICATIONS OF THE INVALIDATION OF THE PRIVACY SHIELD DECISION IN *SCHREMS II*

This Part analyzes the practical implications of the invalidation of the Privacy Shield Decision in *Schrems II*. It first gives an overview of the mechanisms for cross-border transfers of personal data to third countries provided in Chapter V of the GDPR and carves out the challenges companies and other bodies have faced since the invalidation of the Privacy Shield Decision. It then discusses the May 2023 decision of the Irish DPC regarding Meta Platforms Ireland Limited to highlight such challenges.

88 *Schrems I*, ECLI:EU:C:2015:650, ¶ 95.

89 *Schrems II*, ECLI:EU:C:2020:559, ¶ 197.

### A. *Mechanisms for Cross-Border Transfers of Personal Data to Third Countries*

According to Chapter V of the GDPR, personal data can be transferred from the EU to a third country, such as the United States, only under one of the following three conditions[90]: (1) it has been confirmed in an EC adequacy decision that the third country "ensures an adequate level of protection";[91] (2) in the absence of an adequacy decision, "appropriate safeguards" are provided to guarantee the required level of protection under EU law, such as via binding corporate rules (BCRs) or SCCs;[92] or (3) in the absence of an adequacy decision or of appropriate safeguards, the transfers are based on "[d]erogations for specific situations," such as consent or "important reasons of public interest."[93]

The CJEU's *Schrems II* judgment on July 16, 2020, invalidating the Privacy Shield Decision,[94] caused considerable uncertainties and hurdles in lawfully transferring personal data from the EU to the United States. An adequacy decision under Article 45(3) of the GDPR has the advantage that cross-border transfers of personal data from the EU to a third country can take place without the need for additional safeguards or authorizations.[95] According to the EC, an adequacy decision "guarantees the free flow of personal data thus facilitating commercial exchanges with the third country in question."[96] With an adequacy decision in place, it is thus easier to transfer personal data from the EU to a third country, compared to relying on one of the alternative mechanisms provided in Chapter V of the GDPR in its absence. An adequacy decision can also contribute to more transparency, lower costs, and greater legal certainty.

During the nearly three years between the invalidation of the Privacy Shield Decision in *Schrems II* and the adoption of Privacy Shield 2.0, however, companies and other bodies had no choice but to stop cross-border transfers of personal data from the EU to the United States or rely on alternative lawful mechanisms, such as "[t]ransfers subject to appropriate safeguards" under Article 46 of the GDPR or transfers based on "[d]erogations for specific situations" under Article 49 of the GDPR.[97] In particular, in the absence of an adequacy decision, SCCs are the most

---

90 *See* GDPR, *supra* note 3, art. 44.

91 *Id.* art. 45(1).

92 *Id.* art. 46(1).

93 *Id.* art. 49(1).

94 For more information, see *supra* Section I.B.

95 GDPR, *supra* note 3, recital 103, art. 45(1); European Commission Factsheet MEMO/17/15, *supra* note 26.

96 European Commission Factsheet MEMO/17/15, *supra* note 26.

97 GDPR, *supra* note 3, arts. 46, 49.

widely used mechanism for cross-border transfers of personal data from the EU to a third country.[98]

Under Article 46(1) of the GDPR, "a controller or processor may transfer personal data to a third country . . . 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."[99] According to Article 46(2)(c) of the GDPR, such "appropriate safeguards" can be "standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)."[100]

Although the CJEU upheld the validity of the EC SCC Decision in *Schrems II*, the court observed the need for "supplementary measures" to compensate for any lack of data protection.[101] The CJEU stated:

> It follows that the 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 and processors established in the European Union and, consequently, independently of the level of protection guaranteed 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 of protection required under EU law, they may require*, depending on the prevailing position in a particular third country, *the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.*[102]

The court further clarified that:

> 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

98 *See id.* art. 46(1), (2)(c); NIGEL CORY, ELLYSSE DICK & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., THE ROLE AND VALUE OF STANDARD CONTRACTUAL CLAUSES IN EU-U.S. DIGITAL TRADE 1 (2020), https://www2.itif.org/2020-standard-contractual-clauses.pdf [https://perma.cc/C4Q2-KUP9]; CECILIA BONEFELD-DAHL, FRANK HEEMSKERK, MARKUS J. BEYRER & ERIC-MARK HUITEMA, DIGITALEUROPE, *SCHREMS II* IMPACT SURVEY REPORT 5 (2022), https://cdn.digitaleurope.org/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf [https://perma.cc/KN99-HECD].

99 GDPR, *supra* note 3, art. 46(1) (emphasis added).

100 *Id.* art. 46(2)(c).

101 *Schrems II*, ECLI:EU:C:2020:559, ¶ 133.

102 *Id.* (emphasis added).

> providing, where necessary, additional safeguards to those offered by those clauses.[103]

The CJEU did not further specify what these "supplementary measures" could look like, and its finding ultimately has led to significant uncertainty among companies and other bodies about lawfully using SCCs to transfer personal data from the EU to third countries.[104]

Moreover, on June 4, 2021, the EC adopted new SCCs under the GDPR, which must be the basis for personal data transfer agreements concluded *after* September 27, 2021.[105] In particular, the new SCC Decision 2021/914[106] repealed the previous SCC Decisions 2001/497[107] and 2010/87,[108] effective from September 27, 2021.[109] Moreover, entities that relied on the previous SCCs—data transfer agreements concluded *before* September 27, 2021—had to switch to the new SCCs by December 27, 2022, at the latest, which involved significant administrative burdens, time, costs, and hurdles for these entities.[110] This required update has likely also further hampered personal data transfers from the EU to the United States due to delays in switching to the new SCCs.

---

103 *Id.* ¶ 134.

104 For more information on SCCs and the issues caused by *Schrems II*, see, for example, Laura Bradford, Mateo Aboy & Kathleen Liddell, *Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II*, 8 J.L. & BIOSCIENCES, no. 1, Jan.–June 2021, at 1, and Marcelo Corrales Compagnucci, Mateo Aboy & Timo Minssen, *Cross-Border Transfers of Personal Data After* Schrems II*: Supplementary Measures and New Standard Contractual Clauses (SCCs)*, 4 NORDIC J. EUR. L. 37 (2021). The European Data Protection Board adopted recommendations "[t]o help exporters . . . with the complex task of assessing third countries and identifying appropriate supplementary measures where needed." Eur. Data Prot. Bd., *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance With the EU Level of Protection of Personal Data* (June 18, 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [https://perma.cc/7U3F-P3UZ].

105 *See* Eur. Comm'n, The New Standard Contractual Clauses—Questions and Answers Overview 4, 12 (2022), https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf [https://perma.cc/XVM2-AAP2].

106 Commission Implementing Decision 2021/914, 2021 O.J. (L 199) 31 (EU).

107 Commission Decision 2001/497, 2001 O.J. (L 181) 19 (EC).

108 Decision 2010/87—SCC Decision, *supra* note 28.

109 Commission Implementing Decision 2021/914, *supra* note 106, art. 4.

110 *Id.*; Eur. Comm'n, *supra* note 105, at 12.

### B. *The Decision of the Irish DPC in the Matter of Meta Platforms Ireland Limited*

On May 12, 2023, Meta Platforms Ireland Limited (formerly named Facebook Ireland Limited) was fined €1.2 billion because of an infringement of Article 46(1) of the GDPR.[111] The Irish DPC found that:

(i) US law does not provide a level of protection that is essentially equivalent to that provided by EU law;

(ii) Neither the 2010 SCCs nor the 2021 SCCs can compensate for the inadequate protection provided by US law;

(iii) Meta Ireland does not have in place supplemental measures which compensate for the inadequate protection provided by US law; and,

(iv) It is not open to Meta Ireland to rely on the derogations provided for at Article 49(1) GDPR, or any of them, when making the Data Transfers.[112]

On top of the record administrative fine, the Irish DPC also ordered that Meta Platforms Ireland Limited suspend EU-U.S. transfers of personal data between itself and Meta Platforms, Inc. (formerly named Facebook, Inc.) within five months.[113] In addition, Meta Platforms Ireland Limited must "bring its processing operations into compliance with Chapter V [of the] GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR, within 6 (six) months."[114]

---

111 *In re* Meta Platforms Ire. Ltd., Decision of the Data Prot. Comm'n Made Pursuant to Section 111 of the Data Prot. Act, 2018 and Articles 60 and 65 of the GDPR, IN-20-8-1, ¶ 10.2–3(iii) (Ir. Data Prot. Comm'n May 12, 2023), https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf [https://perma.cc/P25W-EKBP].

112 *Id.* ¶ 10.1(i)–(iv).

113 *Id.* ¶¶ 10.3(i), 10.4–10.10; *see also supra* Section I.B.

114 *Meta Platforms Ire. Ltd.*, IN-20-8-1, ¶ 10.3(ii). This order and the administrative fine were imposed following the binding decision of the European Data Protection Board on April 13, 2023. *See* Eur. Data Prot. Bd., *Binding Decision 1/2023 on the Dispute Submitted by the Irish SA on Data Transfers by Meta Platforms Ireland Limited for Its Facebook Service (Art. 65 GDPR)*, ¶ 267 (Apr. 13, 2023), https://edpb.europa.eu/system/files/2023-05/edpb_bindingdecision_202301_ie_sa_facebooktransfers_en.pdf [https://perma.cc/C63K-KMLA] ("On the basis of the above considerations, the EDPB instructs the IE SA [i.e., the Irish DPC] to include in its final decision an order for Meta IE [Meta Platforms Ireland Limited] to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR, within 6 months following the date of notification of the IE SA's final decision to Meta IE."); *id.* ¶ 178 ("[T]he EDPB instructs the IE SA to impose an administrative fine on Meta IE for the infringement of Article 46(1) GDPR that is in line with the principles of effectiveness, proportionality and dissuasiveness under Article 83(1), giving due regard to the relevant aggravating factors under Article 83(2) GDPR, namely the factors

The Irish DPC's decision only binds Meta Platforms Ireland Limited.[115] Still, it had important implications for other companies that transfer personal data from the EU to the United States based on SCCs because they might have also potentially violated the requirements of Chapter V of the GDPR.[116] Meta Platforms Ireland Limited immediately announced that it would not accept this decision.[117] Consequently, this case only underscored the significant legal uncertainties companies and other bodies experienced and the urgent need for the adoption of Privacy Shield 2.0, ultimately rendering the Irish DPC's suspension order obsolete.[118]

---

referred to in Article 83(2)(a), (b), (g), (d), (k) GDPR. When calculating the fine, the IE SA should take into consideration the total turnover of the group of companies headed by Meta Platforms, Inc. for the financial year preceding the adoption of the IE SA's final decision. The IE SA's assessment should be guided by the EDPB Guidelines on calculation of fines and the EDPB's assessment in this Binding Decision."). For the binding decision, see *id.* ¶¶ 268–79.

115 *Meta Platforms Ire. Ltd.*, IN-20-8-1, ¶ 10.11.

116 *See id.* ("It is clear, however, that the analysis in this Decision exposes a situation whereby *any* internet platform falling within the definition of an electronic communications service provider subject to the FISA 702 PRISM programme may equally fall foul of the requirements of Chapter V GDPR and the EU Charter of Fundamental Rights regarding their transfers of personal data to the USA."). On July 4, 2023, the EC also proposed a new Regulation to strengthen enforcement of the GDPR in cross-border cases. *See Proposal for a Regulation of the European Parliament and of the Council Laying Down Additional Procedural Rules Relating to the Enforcement of Regulation (EU) 2016/679*, COM (2023) 348 final (July 4, 2023); European Commission Questions & Answers QANDA/23/3610, Stronger Enforcement of the GDPR in Cross-Border Cases (July 4, 2023), https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3610 [https://perma.cc/8PXL-HPNP].

117 Press Release, Nick Clegg, President, Global Affs. & Jennifer Newstead, Chief Legal Officer, Meta, Our Response to the Decision on Facebook's EU-US Data Transfers (May 22, 2023), https://about.fb.com/news/2023/05/our-response-to-the-decision-on-facebooks-eu-us-data-transfers [https://perma.cc/2BUQ-KQZH]. In June 2023, the Irish court granted Meta Platforms Ireland Limited a stay, stopping the clock on the DPC's suspension order. Justice Denis McDonalds even extended the stay until July 31, 2023. *See* Padraic Halpin & Foo Yun Chee, *EU to Meet on U.S. Data Transfer Pact in Mid-July, Lawyer Says*, REUTERS (June 26, 2023, 4:48 PM), https://www.reuters.com/world/eu-meet-us-data-transfer-pact-mid-july-lawyer-2023-06-26 [https://perma.cc/S8EX-ZT3P]; *Court Continues Stay on Decision That Meta Must Suspend EU-US Data Transfer*, IRISH TIMES (June 26, 2023, 5:49 PM), https://www.irishtimes.com/crime-law/courts/2023/06/26/court-continues-stay-on-decision-that-meta-must-suspend-eu-us-data-transfer [https://perma.cc/QER7-DRJ4].

118 Press Release, Nick Clegg, President, Global Affs. & Jennifer Newstead, Chief Legal Officer, Meta, *supra* note 117; a Meta Company Spokesperson updated the press release on September 7, 2023, stating "Meta will rely on the new Data Privacy Framework (DPF) for the transfer of certain types of data, including Facebook user data and data relating to Meta business tools, from the EU to the US. . . . Notwithstanding this positive development, our appeals against the decisions of the Irish Data Protection Commission and European Data Protection Board continue."

## III. PRIVACY SHIELD 2.0

The U.S. government and the EU made significant yearslong efforts toward the adoption of a new adequacy decision to restore transatlantic data flows and commercial exchanges between the EU and the United States. The following focuses on four relevant events toward the adoption of Privacy Shield 2.0: (1) the announcement of a new Trans-Atlantic Data Privacy Framework; (2) the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities; (3) the EC's draft adequacy decision; and (4) the launch of the adoption process and the ultimate adoption of Privacy Shield 2.0.

### A. *The Announcement of a New Trans-Atlantic Data Privacy Framework*

On March 25, 2022, after more than a year of intensive negotiations, the EU and the United States announced that they generally agreed on a new Trans-Atlantic Data Privacy Framework, expected to be the successor to the invalidated Privacy Shield Decision and thus also known as "Privacy Shield 2.0."[119] According to the joint statement, the new framework would promote cross-border data transfers and address the concerns the CJEU expressed with the Privacy Shield Decision in *Schrems II*.[120]

According to the EC, key principles of the proposed framework would include:

> - [*D*]*ata will be able to flow freely and safely* between the EU and participating U.S. companies
> - . . . A new set of rules and *binding safeguards to limit access to data* by U.S. intelligence authorities to what is *necessary and proportionate* to protect national security; U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
> - . . . *A new two-tier redress system* to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a *Data Protection Review Court* [DPRC]

---

119 Press Release, The White House, United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework (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/V3DA-4LLM].

120 *Id.*

- . . . *Strong obligations for companies* processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce
- . . . *Specific monitoring and review mechanisms*.[121]

The White House also emphasized that the United States committed itself to: "[s]trengthen the privacy and civil liberties safeguards governing U.S. signals intelligence activities; . . . [e]stablish a new redress mechanism with independent and binding authority; and . . . [e]nhance its existing rigorous and layered oversight of signals intelligence activities."[122]

### B. *The Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities*

On October 7, 2022, President Biden signed the awaited Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (EO 14086).[123] This Executive Order, which has the force of law, includes the U.S. commitments promised in the March 2022 announcement of a new Trans-Atlantic Data Privacy Framework and forms the basis of the EC's adequacy decision.[124]

EO 14086 consists of five sections: (1) *Purpose*; (2) *Signals Intelligence Activities*, (3) *Signals Intelligence Redress Mechanism*, (4) *Definitions*, and (5) *General Provisions*.

In particular, section 1 of EO 14086 clarifies that:

---

121 European Commission Factsheet FS/22/2100, *Trans-Atlantic Data Privacy Framework* (Mar. 2022), https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf [https://perma.cc/42PL-VWRR].

122 Press Release, The White House, FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework [https://perma.cc/UKG5-NV5U].

123 Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 7, 2022).

124 *See supra* Section III.A; *infra* Sections III.C–III.D; *What Is an Executive Order?*, AM. BAR ASSOC. (Jan. 25, 2021), https://www.americanbar.org/groups/public_education/publications/teaching-legal-docs/what-is-an-executive-order- [https://perma.cc/HY4R-SUHG]; European Commission Factsheet FS/22/2100, *supra* note 121; Press Release, The White House, *supra* note 119; Press Release, The White House, FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (Oct. 7, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework [https://perma.cc/X36X-X8D2]; European Commission Questions & Answers QANDA/23/3752, *supra* note 18.

> [T]he United States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners. At the same time, the United States recognizes that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information. Therefore, this order establishes safeguards for such signals intelligence activities.[125]

The following two subsections thoroughly examine sections 2 and 3 of EO 14086, which are particularly relevant in response to the common concerns of the CJEU in *Schrems I* and *Schrems II*.[126]

### 1. Signals Intelligence Activities

Section 2 of EO 14086 is composed of five subsections: (a) *Principles*, (b) *Objectives*, (c) *Privacy and civil liberties safeguards*, (d) *Subjecting signals intelligence activities to rigorous oversight*, and (e) *Savings clause*.

Subsection (a) contains principles and, in particular, requires signals intelligence activities to be subject to appropriate safeguards:

> (ii) Signals intelligence activities shall be *subject to appropriate safeguards*, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that:
>
> (A) signals intelligence activities shall be conducted only following a determination, based on a *reasonable assessment of all relevant factors*, that the activities are *necessary* to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and
>
> (B) signals intelligence activities shall be conducted *only to the extent and in a manner that is proportionate* to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and

125 Exec. Order 14086 § 1, 87 Fed. Reg. 62283, 62283 (Oct. 7, 2022).

126 *See supra* Part I.

> civil liberties of all persons, *regardless of their nationality or wherever they might reside*.[127]

Subsection (b) contains a list of twelve "legitimate objectives"; at least one must be pursued for signals intelligence collection activities to be conducted.[128] Examples include "understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, [or] a faction of a foreign nation, . . . in order to protect the national security of the United States and of its allies and partners";[129] "protecting against terrorism, the taking of hostages, and the holding of individuals captive . . . conducted by or on behalf of a foreign government, foreign organization, or foreign person";[130] or "protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person."[131] The U.S. President has the discretion to authorize additional objectives.[132]

Subsection (b) also lists "[p]rohibited objectives," such as suppressing or burdening individuals' criticism or dissent,[133] "suppressing or restricting legitimate privacy interests"[134] or "a right to legal counsel,"[135] or "disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion."[136]

Subsection (c) states, among other things, certain limitations on the bulk collection of signals intelligence. First, "[t]argeted collection shall be prioritized."[137]

Second,

> [w]hen it is *determined to be necessary to engage in bulk collection* in order to advance a validated intelligence priority, the element of the Intelligence Community shall apply *reasonable methods and technical measures* in order to *limit the data collected to only what is necessary*

---

127 Exec. Order 14086 § 2(a)(ii)(A)–(B), 87 Fed. Reg. 62283, 62283 (Oct. 7, 2022) (emphasis added).

128 *Id.* § 2(b)(i)(A)(1)–(12), 87 Fed. Reg. at 62283–84.

129 *Id.* § 2(b)(i)(A)(1), 87 Fed. Reg. at 62284.

130 *Id.* § 2(b)(i)(A)(5), 87 Fed. Reg. at 62284.

131 *Id.* § 2(b)(i)(A)(8), 87 Fed. Reg. at 62284.

132 *Id.* § 2(b)(i)(B), 87 Fed. Reg. at 62284.

133 *Id.* § 2(b)(ii)(A)(1), 87 Fed. Reg. at 62284.

134 *Id.* § 2(b)(ii)(A)(2), 87 Fed. Reg. at 62284.

135 *Id.* § 2(b)(ii)(A)(3), 87 Fed. Reg. at 62284.

136 *Id.* § 2(b)(ii)(A)(4), 87 Fed. Reg. at 62284.

137 *Id.* § 2(c)(ii)(A), 87 Fed. Reg. at 62286.

> to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.[138]

Third, subsection (c) lists six of the above-mentioned objectives and clarifies that "[e]ach element of the Intelligence Community that collects signals intelligence through bulk collection shall use such information only in pursuit of one or more of . . . [such] objectives."[139] Again, the U.S. President has the discretion to authorize additional objectives.[140]

Subsection (c) also contains handling requirements for personal information that is collected via signals intelligence, including

---

138 *Id.* (emphasis added). The terms "'Intelligence Community' and 'elements of the Intelligence Community' shall have the same meaning as they have in Executive Order 12333." *Id.* § 4(g), 87 Fed. Reg. at 62295. The terms "Intelligence Community and elements of the Intelligence Community refer[] to:

> (1) The Office of the Director of National Intelligence;
>
> (2) The Central Intelligence Agency;
>
> (3) The National Security Agency;
>
> (4) The Defense Intelligence Agency;
>
> (5) The National Geospatial-Intelligence Agency;
>
> (6) The National Reconnaissance Office;
>
> (7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
>
> (8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;
>
> (9) The intelligence elements of the Federal Bureau of Investigation;
>
> (10) The Office of National Security Intelligence of the Drug Enforcement Administration;
>
> (11) The Office of Intelligence and Counterintelligence of the Department of Energy;
>
> (12) The Bureau of Intelligence and Research of the Department of State;
>
> (13) The Office of Intelligence and Analysis of the Department of the Treasury;
>
> (14) The Office of Intelligence and Analysis of the Department of Homeland Security;
>
> (15) The intelligence and counterintelligence elements of the Coast Guard; and
>
> (16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community."

Exec. Order 12333, section 3.5(h), as amended by Exec. Orders 13284 (2003), 13355 (2004) and 13470 (2008).

139 Exec. Order 14086 § 2(c)(ii)(B), 87 Fed. Reg. at 62286. Examples include "protecting against terrorism, the taking of hostages, and the holding of individuals captive . . . conducted by or on behalf of a foreign government, foreign organization, or foreign person," *id.* § 2(c)(ii)(B)(1), 87 Fed. Reg. at 62286, or "protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person," *id.* § 2(c)(ii)(B)(4), 87 Fed. Reg. at 62286.

140 *Id.* § 2(c)(ii)(C), 87 Fed. Reg. at 62286.

minimization, data security, access, and quality.[141] In addition, it clarifies that the head of each element of the Intelligence Community (IC element) shall, within one year of the release of the Executive Order (i.e., by October 7, 2023), update the already existing policies and procedures issued in accordance with Presidential Policy Directive 28 (PPD-28)[142] to comply with the privacy and civil liberties safeguards in EO 14086.[143] They should also make the updated policies and procedures publicly available "to the maximum extent possible."[144]

It is worth noting that PPD-28 was partially revoked (except for section 3, section 6, and the classified annex) by the National Security Memorandum issued on the same day as EO 14086.[145] Furthermore, already on July 3, 2023, the Office of the Director of National Intelligence, together with IC elements, released the updated policies and procedures to comply with the privacy and civil liberties safeguards in EO 14086.[146] In total, eleven IC elements' procedures were published, such as those of the Central Intelligence Agency (CIA),[147] the FBI,[148] and the NSA.[149]

---

141 *Id.* § 2(c)(iii), 87 Fed. Reg. at 62286–88.

142 *Presidential Policy Directive—Signals Intelligence Activities*, WHITE HOUSE (Jan. 17, 2014) https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/4L33-XG6N] [hereinafter PPD-28].

143 Exec. Order 14086 § 2(c)(iv)(A)–(B), 87 Fed. Reg. at 62288. The update shall happen "in consultation with the Attorney General, the CLPO [Civil Liberties Protection Officer of the Office of the Director of National Intelligence], and the Privacy and Civil Liberties Oversight Board (PCLOB)." *Id.* § 2(c)(iv)(B), 87 Fed. Reg. at 62288.

144 *Id.* § 2(c)(iv)(C), 87 Fed. Reg. at 62288.

145 Press Release, The White House, National Security Memorandum on Partial Revocation of Presidential Policy Directive 28 (Oct. 7, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28 [https://perma.cc/A96U-WZAQ]; *see* Exec. Order 14086 § 5(f), 87 Fed. Reg. at 62296.

146 Press Release, Off. of the Dir. of Nat'l Intel., ODNI Releases Intelligence Community Procedures Implementing New Safeguards in Executive Order 14086 (July 3, 2023), https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086 [https://perma.cc/UR8M-BE5Y].

147 *Signals Intelligence Activities*, CIA, https://www.intel.gov/assets/documents/702%20Documents/oversight/CIA_EO_14086_Procedures.pdf [https://perma.cc/95JJ-MQ84].

148 Federal Bureau of Investigation Executive Order 14086 Implementing Policies and Procedures, FBI (June 29, 2023), https://www.intel.gov/assets/documents/702%20Documents/oversight/FBI_EO_14086_Procedures_06292023.pdf [https://perma.cc/F3J6-8MGC].

149 (U) NSA/CSS Policy 12-3 Annex C Supplemental Procedures for the Collection, Processing, Querying, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons, NSA (June 29, 2023), https://www.intel.gov/assets/documents/702%20Documents/oversight/NSA_EO_14086_Procedures_Policy_12-3_Annex_C.pdf [https://perma.cc/2RBK-3SLT]; Press Release, Off. of the Dir. of Nat'l Intel., *supra* note 146.

Subsection (d) states additional oversight mechanisms to ensure rigorous oversight of signals intelligence activities. Those mechanisms include having senior-level legal, oversight, and compliance officials in place; employee training requirements; and reporting requirements for significant incidents of noncompliance, as well as remediating and preventing their recurrence.[150]

Subsection (e) contains a savings clause. It clarifies that the Executive Order usually does not limit signals intelligence collection techniques authorized through other applicable laws or presidential directives.[151]

### 2. Signals Intelligence Redress Mechanism

Section 3 of EO 14086 consists of six subsections: (a) *Purpose*, (b) *Process for submission of qualifying complaints*, (c) *Initial investigation of qualifying complaints by the CLPO* (Civil Liberties Protection Officer of the Office of the Director of National Intelligence), (d) *Data Protection Review Court*, (e) *Annual review by PCLOB* (Privacy and Civil Liberties Oversight Board) *of redress process*, and (f) *Designation of qualifying state*.[152]

Subsection (a) clarifies that Section 3 of EO 14086 "*establishes a redress mechanism to review qualifying complaints* transmitted by the appropriate public authority in a qualifying state concerning United States signals intelligence activities for any covered violation of United States law and, if necessary, appropriate remediation."[153]

Subsection (b) contains a requirement that the Director of National Intelligence must establish the process for submitting such complaints within sixty days of the release of the Executive Order.[154] The Director shall thereby consult "with the Attorney General and the heads of elements of the Intelligence Community that collect or handle personal information collected through signals intelligence."[155] Within the sixty-day deadline, on December 6, 2022, the Director of National Intelligence signed Intelligence Community Directive 126 that implements

150 Exec. Order 14086 § 2(d)(i)–(iii), 87 Fed. Reg. at 62289.

151 *Id.* § 2(e), 87 Fed. Reg. at 62289.

152 *Id.* § 3(a)–(f), 87 Fed. Reg. at 62289–94.

153 *Id.* § 3(a), 87 Fed. Reg. at 62289 (emphasis added).

154 *Id.* § 3(b), 87 Fed. Reg. at 62289–90.

155 *Id.*

procedures for the signals intelligence redress mechanism under the Executive Order.[156]

The redress mechanism established in section 3 of EO 14086 has two layers. Subsection (c) explains the first layer of the redress mechanism with the CLPO. It provides that the CLPO shall investigate the qualifying complaint by reviewing the information necessary, determine whether there was a covered violation of U.S. law, and, if so, determine the appropriate remediation.[157] According to subsection (c), the Director of National Intelligence should consult with the Attorney General and establish this process by the CLPO.[158] The Director also fulfilled this obligation by issuing Intelligence Community Directive 126. The CLPO's determination to undertake appropriate remediation is binding for each IC element, including each agency containing an IC element, unless the DPRC determines otherwise.[159] In addition, subsection (c) provides for the independence of the CLPO: "The Director shall not interfere with a review by the CLPO of a qualifying complaint . . . ; nor shall the Director remove the CLPO for any actions taken pursuant to this order, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity."[160]

As the second layer of the redress mechanism, subsection (d) requires the Attorney General to promulgate regulations establishing the DPRC within 60 days of the release of the Executive Order.[161] Attorney General Merrick Garland fulfilled this obligation by signing, on October 7, 2022, the accompanying regulation establishing the DPRC (AG Regulation).[162]

The DPRC is responsible for reviewing the CLPO's determinations.[163] A DPRC panel will be convened consisting of three judges upon receipt of an application from the complainant or an IC element.[164] Individuals to serve as DPRC judges are appointed by the

156 U.S. OFF. OF THE DIR. OF NAT'L INTEL., ICD 126, IMPLEMENTATION PROCEDURES FOR THE SIGNALS INTELLIGENCE REDRESS MECHANISM UNDER EXECUTIVE ORDER 14086 (Dec. 6, 2022), https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf [https://perma.cc/V7U2-2MPN].

157 Exec. Order 14086 § 3(c)(i)(A)–(C), 87 Fed. Reg. at 62290.

158 *Id.* § 3(c)(i), 87 Fed. Reg. at 62290.

159 *Id.* § 3(c)(ii), 87 Fed. Reg. at 62290–91.

160 *Id.* § 3(c)(iv), 87 Fed. Reg. at 62291.

161 *Id.* § 3(d)(i), 87 Fed. Reg. at 62291.

162 *See* 28 C.F.R. pt. 201 (2023) [hereinafter AG Regulation]. The final rule was published on October 14, 2022. *See* Data Protection Review Court, 87 Fed. Reg. 62303 (Oct. 14, 2022) (to be codified at 28 C.F.R. pt. 201).

163 Exec. Order 14086 § 3(d)(i), 87 Fed. Reg. at 62291; 28 C.F.R. § 201.1 (2023).

164 Exec. Order 14086 § 3(d)(i)(B), 87 Fed. Reg. at 62291. For more information on the application for review and convening of panels, see also 28 C.F.R. §§ 201.6, 201.7(a) (2023).

Attorney General, who consults with the Director of National Intelligence, the Secretary of Commerce, and the PCLOB.[165] According to subsection (d), they need to fulfill the following criteria:

> [Individuals to serve as DPRC judges] shall be legal practitioners with appropriate experience in the fields of data privacy and national security law, giving weight to individuals with prior judicial experience, and who shall not be, at the time of their initial appointment, employees of the United States Government. During their term of appointment on the Data Protection Review Court, such judges shall not have any official duties or employment within the United States Government other than their official duties and employment as judges on the Data Protection Review Court.[166]

On November 16, 2023, Attorney General Garland announced eight DRPC judges and formally swore in six of them during a ceremony.[167]

Once the application is received and the DPRC panel convened, the three-judge panel will select a special advocate who will advocate concerning the complainant's interest in the matter, among other things.[168] Subsection (d) also clarifies that "[t]he Data Protection Review Court panel shall *impartially review* the determinations made by the CLPO with respect to whether a covered violation occurred and the appropriate remediation in the event there was such a violation."[169] If the DPRC panel concludes that it disagrees with any of the determinations made by the CLPO, it will issue its own determinations.[170] Upon completion of the review, the DPRC will "inform the complainant, . . . that 'the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation.'"[171]

---

165 Exec. Order 14086 § 3(d)(i)(A), 87 Fed. Reg. at 62291.

166 *Id.* at § 3(d)(i)(A), 87 Fed. Reg. at 62291. For more information on the appointment of judges, see also 28 C.F.R. § 201.3 (2023).

167 Two judges could not attend the ceremony in person; Press Release, Off. Pub. Affs., Attorney General Merrick B. Garland Announces Judges of the Data Protection Review Court, https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court [https://perma.cc/CXH6-BT93] (last updated Nov. 14, 2023). The eight DPRC judges are James E. Baker, Rajesh De, James X. Dempsey, Mary B. DeRosa, Thomas B. Griffith, Eric H. Holder, Jr., David F. Levi, and Virginia A. Seitz; Off. Priv. and C.L., The Data Protection Review Court (Nov. 14, 2023), https://www.justice.gov/opcl/redress-data-protection-review-court [https://perma.cc/UQ27-F6JB].

168 Exec. Order 14086 § 3(d)(i)(C), 87 Fed. Reg. at 62291. For more information on special advocates, see also 28 C.F.R. §§ 201.4, 201.8 (2023).

169 Exec. Order 14086 § 3(d)(i)(D), 87 Fed. Reg. at 62291 (emphasis added). For more information on the DPRC panel's review, see also 28 C.F.R. § 201.9 (2023).

170 Exec. Order 14086 § 3(d)(i)(E), 87 Fed. Reg. at 62292.

171 *Id.* at § 3(d)(i)(H), 87 Fed. Reg. at 62292.

The DPRC panel's determinations to undertake appropriate remediation, such as the deletion of the data, are binding and each IC element, including each agency containing an IC element, must comply with them.[172] Subsection (d) also states the independence of the DPRC:

> The Attorney General shall not interfere with a review by a Data Protection Review Court panel of a determination the CLPO made regarding a qualifying complaint . . . ; nor shall the Attorney General remove any judges appointed . . . , or remove any judge from service on a Data Protection Review Court panel, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity, after taking due account of the standards in the Rules for Judicial-Conduct and Judicial-Disability Proceedings promulgated by the Judicial Conference of the United States pursuant to the Judicial Conduct and Disability Act (28 U.S.C. 351 et seq.).[173]

Subsection (e) encourages the PCLOB to conduct an annual review of the redress process.[174] The review should also include, among other things, whether the CLPO and the DPRC are operating consistently with the Executive Order and whether the IC elements have fully complied with the CLPO's and DPRC's determinations.[175] On October 7, 2022, the PCLOB accepted that it would conduct such reviews.[176]

Subsection (f) regulates the designation of qualifying states. It clarifies that "the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism."[177] On June 30, 2023, the Attorney

---

172 *Id.* at § 3(d)(ii), 87 Fed. Reg. at 62292; *see also* 28 C.F.R. § 201.9(g) (2023) ("The decision of each DPRC panel shall be final and binding with respect to the application for review before it and shall be controlling only as to that application for review."); European Commission Questions & Answers QANDA/23/3752, *supra* note 18.

173 Exec. Order 14086 § 3(d)(iv), 87 Fed. Reg. at 62292.

174 *Id.* at § 3(e)(i), 87 Fed. Reg. at 62293.

175 *Id.* at § 3(e)(i), 87 Fed. Reg. at 62293.

176 Press Release, Priv. and C.L. Oversight Bd., Privacy and Civil Liberties Oversight Board Statement Regarding Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (Oct. 7, 2022), https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf [https://perma.cc/7GQ4-4AQM].

177 Exec. Order 14086 § 3(f)(i), 87 Fed. Reg. at 62293. The Attorney General needs to determine:

> [I]n consultation with the Secretary of State, the Secretary of Commerce, and the Director [of National Intelligence], that:
>
> (A) the laws of the country, the regional economic integration organization, or the regional economic integration organization's member countries require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or a member country of the regional economic integration organization;

General, in consultation with the Director of National Intelligence, the Secretary of Commerce, and the Secretary of State, designated the EU, as well as Iceland, Liechtenstein, and Norway, as "qualifying states" under EO 14086.[178] The designation became effective with the adoption of Privacy Shield 2.0 on July 10, 2023, thus permitting EEA individuals to submit complaints under the new redress mechanism.[179] They can submit the complaint to the national data protection authority, which will then refer it to the European Data Protection Board (EDPB), which will forward the complaint to the competent U.S. authorities.[180] A valid complaint does not require the individual to demonstrate that U.S. intelligence agencies, in fact, collected their personal data.[181]

### C. *The EC's Draft Adequacy Decision*

EO 14086, including its accompanying AG Regulation establishing the DPRC, formed the basis of the draft adequacy decision that the EC

---

> (B) the country, the regional economic integration organization, or the regional economic integration organization's member countries of the regional economic integration organization permit, or are anticipated to permit, the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; and
>
> (C) such designation would advance the national interests of the United States.

Exec. Order 14086 § 3(f)(i)(A)–(C), 87 Fed. Reg. at 62293–94.

178 OFF. OF THE ATT'Y GEN., DESIGNATION PURSUANT TO SECTION 3(F) OF EXECUTIVE ORDER 14086, https://www.justice.gov/d9/2023-07/Attorney%20General%20Designation%20Pursuant%20to%20Section%203%28f%29%20of%20Executive%20Order%2014086%20of%20the%20EU%20EEA.pdf [https://perma.cc/2AUS-ZUV3]. For the Supporting Memorandum, see OFF. OF THE ASSISTANT ATT'Y GEN., MEMORANDUM IN SUPPORT OF DESIGNATION OF THE EUROPEAN UNION AND ICELAND, LIECHTENSTEIN AND NORWAY AS QUALIFYING STATES UNDER EXECUTIVE ORDER 14086, https://www.justice.gov/d9/2023-07/Supporting%20Memorandum%20for%20the%20Attorney%20General%27s%20designation%20of%20EU-EEA.pdf [https://perma.cc/ZX37-L948].

179 OFF. OF THE ATT'Y GEN., *supra* note 178; *Executive Order 14086*, U.S. DEP'T OF JUST. (July 2023), https://www.justice.gov/opcl/executive-order-14086 [https://perma.cc/8RUN-R99D]. For the adoption of Privacy Shield 2.0, see *infra* Section III.D.4.

180 Eur. Data Prot. Bd., *Information Note on Data Transfers Under the GDPR to the United States After the Adoption of the Adequacy Decision on 10 July 2023*, at 2 (July 18, 2023), https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-transfers-under-gdpr-united-0_en [https://perma.cc/7K7F-EDM4]; European Commission Questions & Answers QANDA/23/3752, *supra* note 18.

181 *Information Note on Data Transfers Under the GDPR to the United States After the Adoption of the Adequacy Decision on 10 July 2023*, *supra* note 180, at 3; European Commission Questions & Answers QANDA/23/3752, *supra* note 18.

proposed on December 13, 2022.[182] In the introduction of the draft adequacy decision, the EC makes the following finding:

> The Commission has carefully analysed U.S. law and practice, including EO 14086 and the AG Regulation. Based on the findings . . . , the Commission concludes that *the United States ensures an adequate level of protection for personal data* transferred under the EU-U.S. DPF [Data Privacy Framework] from a controller or a processor in the Union . . . to certified organisations in the United States.[183]

The Commission further explains that "[t]his Decision has the effect that personal data transfers from controllers and processors in the Union to certified organisations in the United States may take place without the need to obtain any further authorisation."[184]

Article 1 of the draft adequacy decision then summarizes the EC's conclusion stating that:

> For the purpose of Article 45 of Regulation (EU) 2016/679 [GDPR], the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I.[185]

But in its conclusion, the EC also clarifies:

> Given that the limitations, safeguards and redress mechanism established by EO 14086 are essential elements of the U.S. legal framework on which the Commission's assessment is based, the *entry into force of this Decision is conditional* upon the *adoption of updated policies and procedures to implement EO 14086 by all U.S. intelligence agencies* and the *designation of the Union as a qualifying organisation* for the purpose of the redress mechanism.[186]

As seen above, the Attorney General designated the EU, Iceland, Liechtenstein, and Norway as "qualifying states" on June 30, 2023.[187] Moreover, the updated policies and procedures of the IC elements were

---

182 Draft Adequacy Decision, *supra* note 31. For more information on EO 14086 and the AG Regulation, see *supra* Section III.B.

183 Draft Adequacy Decision, *supra* note 31, recital 7 (emphasis added).

184 *Id.* recital 8.

185 *See also id.* recital 193 ("The Commission considers that the United States – through the Principles issued by the U.S. DoC [Department of Commerce]—ensures a level of protection for personal data transferred from the Union to certified organisations in the United States under the EU-U.S. Data Privacy Framework that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679").

186 *Id.* recital 196 (emphasis added).

187 *See supra* Section III.B.2.

released on July 3, 2023.[188] Thus, those two key steps further cleared the way toward the adoption of Privacy Shield 2.0 on July 10, 2023.[189]

### D. *The Launch of the Adoption Process and the Ultimate Adoption of Privacy Shield 2.0*

With the release of the draft adequacy decision, the EC also launched its adoption process.[190] The adoption process consists of the following steps: first, the draft adequacy decision is sent to the EDPB to get its opinion,[191] and then a positive vote must be obtained from a committee composed of representatives of the EU Member States.[192] In addition, the European Parliament has the opportunity to, at any time, assert its right of scrutiny over adequacy decisions.[193] Only when these steps have been taken can the EC adopt Privacy Shield 2.0. Then, according to the EC, "data will be able to flow freely and safely between the EU and U.S. companies certified by the Department of Commerce under the new framework."[194]

The following discusses the relevant steps of the adoption process in the chronological order in which they happened, namely: (1) the EDPB's opinion, (2) the European Parliament's opinion, (3) the committee's vote, and (4) the EC's adoption of its adequacy decision.

#### 1. The EDPB's Opinion

On the day of its publication on December 13, 2022, the draft adequacy decision was forwarded to the EDPB for its opinion.[195] The

---

188 *See supra* Section III.B.1.

189 *See infra* Section III.D.

190 European Commission Questions & Answers QANDA/22/6045, EU-U.S. Data Privacy Framework (Oct. 7, 2022), https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045 [https://perma.cc/5TRK-39YR]; European Commission Press Release IP/22/7631, Data Protection: Commission Starts Process to Adopt Adequacy Decision for Safe Data Flows with the US (Dec. 13, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631 [https://perma.cc/MBL6-DLYU].

191 European Commission Questions & Answers QANDA/22/6045, *supra* note 190; GDPR, *supra* note 3, art. 70(1)(s).

192 European Commission Questions & Answers QANDA/22/6045, *supra* note 190; *see* GDPR, *supra* note 3, art. 93; Regulation 182/2011, art. 5, 2011 O.J. (L 55) 13 (EU), 15–16 [hereinafter Comitology Regulation].

193 European Commission Questions & Answers QANDA/22/6045, *supra* note 190; Comitology Regulation, *supra* note 192, art. 11.

194 European Commission Questions & Answers QANDA/22/6045, *supra* note 190.

195 *Id.*

EDPB then issued its opinion on February 28, 2023.[196] In a press release published on the same day as the opinion, the EDPB applauded the new requirements incorporating the principles of proportionality and necessity in EO 14086, as well as the establishment of the new redress mechanism.[197] However, the EDPB also expressed concerns about "certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the practical functioning of the redress mechanism."[198] The press release then goes on to say:

> The EDPB would welcome if not only the entry into force but also the adoption of the decision were conditional upon the adoption of updated policies and procedures to implement Executive Order 14086 by all U.S. intelligence agencies. The EDPB recommends the Commission to assess these updated policies and procedures and share its assessment with the EDPB.[199]

Moreover, for example, in its opinion, the EDPB highlights:

> While the EDPB recognises that the EO 14086 introduces the concepts of necessity and proportionality in the legal framework of signals intelligence, it underlines the need to closely monitor the effects of these amendments in practice, including the review of internal policies and procedures implementing the EO's safeguards at agency level.[200]

In particular, the EDPB is concerned about the bulk collection of data:

> As a deficit in the current framework, the EDPB has in particular identified that the U.S. legal framework, when allowing for the collection of bulk data under Executive Order 12333, *lacks the requirement of prior authorisation by an independent authority*, as required in the most recent jurisprudence of the EctHR [European

196 Eur. Data Prot. Bd., *Opinion 5/2023 of the European Data Protection Board on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data Under the EU-US Data Privacy Framework* (Feb. 28, 2023), https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [https://perma.cc/WEN6-D9J3] [hereinafter *European Data Protection Board Opinion 5/2023*].

197 *Id.* at 4; European Data Protection Board Press Release, EDPB Welcomes Improvements under the EU-U.S. Data Privacy Framework, but Concerns Remain (Feb. 28, 2023), https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en [https://perma.cc/FR2G-CZK4].

198 European Data Protection Board Press Release, *supra* note 197.

199 *Id.*; *European Data Protection Board Opinion 5/2023*, *supra* note 196, at 4. As seen above, the policies and procedures of the IC elements were updated on July 3, 2020, and thus before the adoption of Privacy Shield 2.0. *See supra* Section III.B.1.

200 *European Data Protection Board Opinion 5/2023*, *supra* note 196, at 5.

> Court of Human Rights], *nor does it provide for a systematic independent review ex post by a court or an equivalently independent body.*[201]

With regard to the new redress mechanism, the EDPB highlights the significant improvements compared to the previous ombudsperson mechanism.[202] However, at the same time, the EDPB is worried "about the general application of the standard response of the DPRC notifying the complainant that either no covered violations were identified or a determination requiring appropriate remediation was issued, and its non-appealability, taken together."[203]

### 2. The European Parliament's Opinion

On February 14, 2023, the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs (LIBE) issued a Draft Motion for a Resolution on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), finding "that the EU-US Data Privacy Framework fails to create actual equivalence in the level of protection."[204] The LIBE Committee thus "calls on the Commission to continue negotiations with its US counterparts with the aim of creating a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU" and "urges the Commission not to adopt the adequacy finding."[205]

The LIBE Committee seems to have concerns that EO 14086 does not meet the standards of Article 7 (right to respect for private life) and Article 8 (right to protection of personal data) of the Charter mainly because:

> [T]he EO requires that signals intelligence must be conducted in a manner proportionate to the 'validated intelligence priority', which appears to be a broad interpretation of proportionality;
>
> . . . the EO does not prohibit the bulk collection of data by signals intelligence . . . [and] the list of legitimate national security

---

201 *Id.* (emphasis added).

202 *Id.* For more information on the ombudsperson mechanism, see *supra* Section I.B.

203 *European Data Protection Board Opinion 5/2023*, *supra* note 196, at 5.

204 Draft Motion for a Resolution, EUR. PARL. DOC. (RSP 2501), ¶ 11 (2023), https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf [https://perma.cc/4V8Q-M5PU].

205 *Id.*

> objectives can be expanded by the US President, who can determine not to make the relevant updates public . . . .[206]

Moreover, according to the LIBE Committee, the DPRC does not meet the standards of Article 47 (the right to effective judicial protection) of the Charter for the following reasons:

> [T]he decisions of the Data Protection Review Court ('DPRC') will be classified and not made public or available to the complainant; . . . the DPRC is part of the executive branch and not the judiciary; . . . a complainant will be represented by a 'special advocate' designated by the DPRC, for whom there is no requirement of independence; . . . the redress process provided by the EO is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data; [and] . . . the proposed redress process does not provide for an avenue for appeal in a federal court and therefore, among other things, does not provide any possibility for the complainant to claim damages . . . .[207]

On April 13, 2023, the European Parliament's LIBE Committee adopted the draft motion for a resolution with amendments.[208] With thirty-seven votes in favor, twenty-one abstaining, and zero against, the Committee concluded that "[t]he proposed EU-U.S. Data Privacy Framework is an improvement, but not enough to justify an adequacy decision on personal data transfers."[209]

On May 11, 2023, the European Parliament adopted the motion for a resolution with further amendments.[210] With 306 votes in favor, 231

---

206 *Id.* ¶¶ 2–3. For more information on Articles 7 and 8 of the Charter, see *supra* Part I.

207 Draft Motion for a Resolution, EUR. PARL. DOC., *supra* note 204, ¶ 5. For more information on Article 47 of the Charter, see *supra* Part I.

208 European Parliament Press Release, MEPs against Greenlighting Personal Data Transfers With the U.S. Under Current Rules (Apr. 13, 2023), https://www.europarl.europa.eu/news/en/press-room/20230411IPR79501/meps-against-greenlighting-data-transfers-with-the-u-s-under-current-rules [https://perma.cc/A7KR-WEDE] [hereinafter Greenlighting Personal Data Transfers Press Release]; Amendments 1-92, EUR. PARL. DOC. (RSP 2501) (2023) https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/AM/2023/04-13/1274535EN.pdf [https://perma.cc/7273-HAVV]; Draft Compromise Amendments, EUR. PARL. DOC. (2023), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2023/04-13/DPFresolution-draftCAs_EN.pdf [https://perma.cc/X7QE-DFCF].

209 Greenlighting Personal Data Transfers Press Release, *supra* note 208.

210 Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, EUR. PARL. DOC. (P9_TA 0204) (2023), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.pdf [https://perma.cc/DB6L-3R8X]; EUR. PARL. DOC. (B9-0234/1) (2023), https://www.europarl.europa.eu/doceo/document/B-9-2023-0234-AM-001-010_EN.pdf [https://perma.cc/QZQ6-B9CE]; EUR. PARL. DOC. (B9-0234/11) (2023),

abstaining, and 27 against, the European Parliament "call[ed] on the Commission not to adopt the adequacy finding until all the recommendations made in this resolution and the EDPB opinion are fully implemented."[211]

### 3. The Committee's Vote

Opinions of the EDPB and the European Parliament are nonbinding.[212] However, they may still influence the EC to amend draft adequacy decisions before seeking the green light from the committee composed of the EU Member States' representatives.[213] To receive the committee's green light, a positive response from at least fifty-five percent of EU Member States (i.e., fifteen out of twenty-seven), representing at least sixty-five percent of the EU population, is needed.[214]

On July 6, 2023, the EC received a green light from the committee. Twenty-four EU Member States voted in favor of a revised version of the draft adequacy decision, with three abstentions.[215] Although the EC made changes to the draft adequacy decision before seeking the opinion of the

---

https://www.europarl.europa.eu/doceo/document/B-9-2023-0234-AM-011-015_EN.pdf [https://perma.cc/3SSL-K4UY].

211 Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 19; European Parliament Press Release, Resolution on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework (May 11, 2023), https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1744353&t=e&l=en [https://perma.cc/LYK6-7ALU].

212 Davinia Brennan, *European Commission Publishes Draft Adequacy Decision for EU-US Data Transfers*, MATHESON (Dec. 15, 2022), https://www.matheson.com/insights/detail/european-commission-publishes-draft-adequacy-decision-for-eu-us-data-transfers [https://perma.cc/BPX9-P3SH]; Kirk J. Nahra, Martin Braun, Shannon Togawa Mercer, Ali A. Jessani & Genesis Ruano, *European Commission Announces Draft U.S. Adequacy Decision*, WILMERHALE (Dec. 15, 2022), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20221215-european-commission-announces-draft-us-adequacy-decision [https://perma.cc/5Y66-AZE8]; Luca Tosoni, *Article 93. Committee Procedure*, *in* THE EU GENERAL DATA PROTECTION REGULATION: A COMMENTARY 271, 272 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds., 2021).

213 *See* Tosoni, *supra* note 212, at 271–72.

214 Brennan, *supra* note 212; Kirk J. Nahra, Martin Braun, Shannon Togawa Mercer, Ali A. Jessani & Genesis Ruano, *supra* note 212; *see also* Comitology Regulation, *supra* note 192, art. 5(1); Consolidated Version of the Treaty on European Union art. 16, ¶ 4, Oct. 26, 2012, 2012 O.J. (C 326), 13 [hereinafter TEU]; TFEU, *supra* note 40, art. 238 ¶ 3.

215 Eur. Comm'n Comitology Reg., *Formal Results of Voting on Revised Draft Commission Implementing Decision Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework* (July 6, 2023), https://ec.europa.eu/transparency/comitology-register/screen/documents/091061/1/consult?lang=en.

committee, these were not material in substance.[216] This is because no changes were made to EO 14086, which forms the basis of Privacy Shield 2.0 and is at the root of the concerns expressed by the EDPB and the European Parliament.[217] The most significant steps taken before the committee's vote were arguably the Attorney General's designation of the EU, Iceland, Liechtenstein, and Norway as "designated states" under section 3(f) of EO 14086, as well as the release of the updated policies and procedures of the IC elements.[218] However, although an option,[219] the EC did *not* use the EDPB and European Parliament's concerns to pressure the United States to make further changes to address them.

### 4. The EC's Adoption of Its Adequacy Decision

Four days after receiving the positive vote from the committee, on July 10, 2023, the EC adopted its adequacy decision (Privacy Shield 2.0), which came into force on the same day.[220] In its adequacy decision, the EC concludes:

> For the purpose of Article 45 of Regulation (EU) 2016/679 [the GDPR], the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I.[221]

With the adoption of Privacy Shield 2.0, any EEA private or public entity can now transfer personal data to United States companies certified under the new framework without the need to put in place further data protection safeguards.[222] Companies can self-certify to the U.S. Department of Commerce by committing to comply with a specific set of

---

216 *Compare* Draft Adequacy Decision, *supra* note 31, *with* Adequacy Decision—Privacy Shield 2.0, *supra* note 17.

217 For a further discussion on the issues of Privacy Shield 2.0, see *infra* Section IV.

218 *See supra* Sections III.B.1–2.

219 Rosa Barcelo, Romain Perray, David P. Saunders & Simon Mortier, *EU-US Transatlantic Data Flows Framework: EU Supervisors Shine Light at the End of the Tunnel*, MCDERMOTT WILL & EMERY (Mar. 9, 2023), https://www.mwe.com/insights/eu-us-transatlantic-data-flows-framework-eu-supervisors-shine-light-at-the-end-of-the-tunnel [https://perma.cc/L2J9-VUJL].

220 Adequacy Decision—Privacy Shield 2.0, *supra* note 17; European Commission Questions & Answers QANDA/23/3752, *supra* note 18.

221 Adequacy Decision—Privacy Shield 2.0, *supra* note 17, art. 2 ¶ 91.

222 European Commission Press Release IP/23/3721, *supra* note 18; European Commission Questions & Answers QANDA/23/3752, *supra* note 18; GDPR, *supra* note 3, art. 45.

privacy principles, such as data minimization.[223] While the U.S. Department of Commerce monitors certified U.S. companies' compliance with the principles, the U.S. Federal Trade Commission is responsible for the enforcement.[224]

In cases where personal data is transferred from the EU to U.S. entities that are *not* included in the Data Privacy Framework List, the benefits of the adequacy decision do *not* apply.[225] Those transfers must rely on alternative lawful mechanisms, such as SCCs.[226] However, the new U.S. national security safeguards, including the redress mechanism, apply notwithstanding the used transfer tool and thus also to such transfers.[227] Thus, data exporters should take the EC's finding in its adequacy decision into account when assessing the effectiveness of the selected transfer tool under Article 46 of the GDPR.[228]

The first evaluation of the EC's finding will be due within one year of the adequacy decision's entry into force.[229] The EC will need to review its conclusion that the United States ensures an adequate level of protection, together with representatives of the competent U.S. and European data protection authorities.[230] Subsequent reviews will be periodic but at least every four years.[231]

---

223 The set of privacy principles includes "the 'EU-U.S. Data Privacy Framework Principles', including the Supplemental Principles (together: the Principles)—issued by the U.S. Department of Commerce (DoC) and contained in Annex I to this [Adequacy] Decision." Adequacy Decision—Privacy Shield 2.0, *supra* note 17, recital 9; European Commission Questions & Answers QANDA/23/3752, *supra* note 18.

224 European Commission Press Release IP/23/3721, *supra* note 18; European Commission Questions & Answers QANDA/23/3752, *supra* note 18.

225 *Information Note on Data Transfers Under the GDPR to the United States After the Adoption of the Adequacy Decision on 10 July 2023*, *supra* note 180, at 2.

226 *Id.* GDPR, *supra* note 3, art. 46. For more information on alternative lawful mechanisms, see *supra* Section II.A.

227 *Information Note on Data Transfers Under the GDPR to the United States After the Adoption of the Adequacy Decision on 10 July 2023*, *supra* note 180, at 2; European Commission Questions & Answers QANDA/23/3752, *supra* note 18.

228 *Information Note on Data Transfers Under the GDPR to the United States After the Adoption of the Adequacy Decision on 10 July 2023*, *supra* note 180, at 2 (citing Adequacy Decision—Privacy Shield 2.0, *supra* note 17, recitals 6–7).

229 European Commission Press Release IP/23/3721, *supra* note 18; Adequacy Decision—Privacy Shield 2.0, *supra* note 17, art. 3(4).

230 *See* sources cited *supra* note 229.

231 Adequacy Decision—Privacy Shield 2.0, *supra* note 17, art. 3(4); GDPR, *supra* note 3, art. 45(3).

## IV. DISCUSSION AND SUGGESTIONS

This Part further analyzes the content of EO 14086 to explore whether, and to what extent, the United States was successful in striking a proper balance between protecting national security and that of U.S. partners and allies and the privacy interests of individuals to satisfy Article 45(1) of the GDPR and the CJEU's concerns in *Schrems I* and *Schrems II*, and thus to have an essentially equivalent level of data protection to what is guaranteed in the EU.[232] It focuses first on a discussion of the principles of necessity and proportionality and then on the new redress mechanism. Finally, it explores the benefits of a comprehensive U.S. federal privacy law.

### A. *The Principles of Necessity and Proportionality*

There is no doubt that the changes introduced by EO 14086 are a step in the right direction in improving safeguards for signals intelligence activities compared to PPD-28, which was partially revoked by the National Security Memorandum of October 7, 2022.[233] As explained in Section III.B.1 of this Article, EO 14086 requires signals intelligence activities to be subject to appropriate safeguards.[234] In particular, EO 14086 clarifies that signals intelligence activities may only be conducted when they are "necessary" and "to the extent and in a manner that is proportionate."[235] EO 14086 also contains twelve objectives, one of which must be at least fulfilled for signals intelligence collection activities to be legitimate.[236] These changes are certainly an improvement to the revoked section 1 of PPD-28, which did not explicitly limit the conduct of signals intelligence activities to the principles of necessity and proportionality but rather required them to "be as tailored as feasible."[237]

Moreover, EO 14086 also introduced stronger safeguards with regard to the bulk collection of signals intelligence. As seen in Section III.B.1 of this Article, the bulk collection of signals intelligence is limited in three ways: (1) a determination that the necessary information cannot reasonably be acquired by targeted collection, (2) the data collected is limited "to only what is necessary," and (3) one of the six listed objectives

232 Exec. Order 14086 § 1, 87 Fed. Reg. at 62283; GDPR, *supra* note 3, recital 104.

233 *See supra* Section III.B.1.

234 Exec. Order 14086 § 2(a)(ii), 87 Fed. Reg. at 62283.

235 *Id.* § 2(a)(ii)(A)–(B), 87 Fed. Reg. at 62283.

236 *Id.* § 2(b)(i)(A)(1)–(12), 87 Fed. Reg. at 62283–84.

237 PPD-28, *supra* note 142, § 1(d).

must be fulfilled to use such information.[238] Although the revoked section 2 of PPD-28 already listed permissible uses of signals intelligence collected in bulk, it did not mention that targeted collection is to be prioritized over bulk collection nor the principle of necessity.

However, essential concerns remain despite these significant improvements introduced by EO 14086. In particular, the abovementioned changes will likely not be enough to comply with the GDPR's requirements, read in the light of Article 7 (right to respect for private life) and Article 8 (right to protection of personal data) of the Charter. There are three main reasons for this assessment.

First, although the explicit incorporation of the principles of necessity and proportionality in EO 14086 is an improvement, this change likely does not go far enough. The issue is that signal intelligence activities may "only" be conducted when they are "necessary *to advance a validated intelligence priority*" and "to the extent and in a manner that is proportionate *to the validated intelligence priority* for which they have been authorized."[239] However, this U.S. interpretation seems to be too broad and inconsistent with the CJEU's interpretation.[240] The principles of necessity and proportionality are *not* being interpreted here in the context of EU law and legal traditions but instead those of the United States.[241] However, this is a problem because there is no harmonized understanding of the meaning of the terms "necessary" and "proportionate" in the United States and the EU.[242] To use Schrems's words:

> The EU and the US now agree on the use of the word 'proportionate' but seem to disagree on the meaning of it. In the end, the CJEU's definition will prevail - likely killing any EU decision again. The European Commission is turning a blind eye on US law again and allowing the continued surveillance of Europeans.[243]

Second, the same issue applies to the bulk collection of signals intelligence. EO 14086 likewise states that the information must be "necessary *to advance a validated intelligence priority*,"[244] which seems to be an overly broad interpretation based on U.S. law and legal traditions. Moreover, the permissibility of bulk collection of signals intelligence

---

238 Exec. Order 14086 § 2(c)(ii)(A)–(B), 87 Fed. Reg. at 62286.

239 *Id.* at § 2(a)(ii)(A)–(B), 87 Fed. Reg. at 62283 (emphasis added).

240 *See also* Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 2.

241 *Id.*

242 *New US Executive Order Unlikely to Satisfy EU Law*, NOYB (Oct. 7, 2022), https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law [https://perma.cc/QV7G-44DK].

243 *Id.* (quoting Schrems).

244 Exec. Order 14086 § 2(c)(ii), 87 Fed. Reg. at 62286 (emphasis added).

generally only requires an IC element's determination that the necessary information cannot reasonably be acquired by targeted collection and is *not* dependent upon an independent authority's prior authorization.[245]

Third, the objectives listed in EO 14086 for both conducting signals intelligence collection activities and using signals intelligence collected in bulk are not exhaustive.[246] Rather, the U.S. President has complete discretion on whether to add objectives for which signals intelligence collection activities or bulk collection may be used.[247] In addition, there is no public release of the updated list of objectives needed if the U.S. President decides against it due to a risk to the U.S. national security.[248]

To sum up, it is *not* unlikely that the CJEU would invalidate Privacy Shield 2.0 in a possible *Schrems III* case on the grounds that the United States fails to ensure an adequate level of protection under Article 45 of the GDPR, read in light of Articles 7 and 8 of the Charter. Schrems already announced on July 10, 2023, that "*noyb* [an Association initiated by Schrems] will challenge the decision."[249] In addition, on September 6, 2023, Philippe Latombe, a French politician, instituted proceedings against Privacy Shield 2.0 before the CJEU under Article 263 of the TFEU.[250] Latombe clarified in a press release that he was challenging the new adequacy decision in his capacity as an EU citizen (not as a politician) whose rights were violated.[251] He asked the CJEU to suspend or even annul Privacy Shield 2.0.[252] Among other things, Latombe claims:

> The text resulting from these negotiations violates the Charter of Fundamental Rights of the European Union, *due to insufficient guarantees of respect for private and family life with regard to the bulk collection of personal data*, and the General Data Protection

---

245 *European Data Protection Board Opinion 5/2023*, *supra* note 196, at 5; *see* Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶¶ 3–4.

246 Exec. Order 14086 § 2(b)(i)(A)(1)–(12), (c)(ii)(B)(1)–(6), 87 Fed. Reg. at 62283–84, 62286.

247 *Id.* at § 2(b)(i)(B), (c)(ii)(C), 87 Fed. Reg. at 62284, 62286.

248 *Id.*; *see* Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 2.

249 *New Trans-Atlantic Data Privacy Framework Largely a Copy of "Privacy Shield"*. Noyb *Will Challenge the Decision*, NOYB (July 10, 2023), https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu [https://perma.cc/GAG9-SWLG].

250 Press Release, Philippe Latombe, Député de la Vendée, Communiqué de Presse, at 1 (Sept. 2023) [hereinafter Philippe Latombe Official Press Release], https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf [https://perma.cc/H2JC-2G5R]. For an unofficial translation from French to English, see Press Release, Philippe Latombe, Member for Vendée, Assemblée Nationale [hereinafter Philippe Latombe Press Release Unofficial English Translation], https://media.licdn.com/dms/document/media/D561FAQE9d0feyqcHkg/feedshare-document-pdf-analyzed/0.1694114846432?e=1696464000&v=beta&t=rMS5V2z26IIdHjVu5gPI_vCPu19tGMye-z-0N0T9_pw [https://perma.cc/X75B-BT8N]; TFEU, *supra* note 40, art. 263.

251 Philippe Latombe Official Press Release, *supra* note 250, at 1.

252 *Id.* at 1–2.

> Regulation (GDPR), due to the *absence of guarantees of a right to an effective remedy and access to an impartial tribunal*, the lack of a framework for automated decisions or lack of guarantees relating to the security of the data processed . . . .[253]

Latombe chose a different procedural route than Schrems pursued in *Schrems I* and *Schrems II*. If successful, Article 263 of the TFEU could be a faster way to achieve Latombe's goal than waiting for a cross-border transfer of personal data under the new framework he could challenge.[254] However, the chosen path also has a high threshold: to make the CJEU review the legality of Privacy Shield 2.0, Latombe must demonstrate standing, which means he must show that the adequacy decision "is of direct concern to" him.[255] On October 12, 2023, the CJEU dismissed Latombe's application for interim measures because he failed to demonstrate serious harm.[256] Thus, Latombe's application for interim measures was rejected based on a lack of urgency and did not prejudge the case's merits, which remains pending.[257]

In the meantime, Schrems is preparing his next move. He will likely challenge a transfer of personal data from the EEA to the United States under Privacy Shield 2.0 in the next months.[258] Thus, *Schrems III* might already be before the CJEU by the beginning of 2024.[259] Schrems's action would be separate and additional to Latombe's proceedings.[260]

---

253 *Id.* at 2 (emphasis added).

254 *See* Philippe Latombe Press Release Unofficial English Translation, *supra* note 250, at 2 (noting that "it offers the considerable advantage of speed").

255 TFEU, *supra* note 40, art. 263, ¶ 4.

256 Case T-553/23 R, Latombe v. European Commission ¶¶ 32–33, https://curia.europa.eu/juris/document/document.jsf?text=&docid=278542&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=225583 (Oct. 12, 2023); *see also* TFEU, *supra* note 40, arts. 278, 279.

257 Case T-553/23 R, Latombe v. European Commission, *supra* note 256, ¶¶ 32–33; *see also* @GChampeau, X, https://twitter.com/gchampeau/status/1712453235020100059 ("Il ne se prononce que sur "l'absence d'urgence" et donc rejette la demande de sursis. L'affaire reste pendante au fond . . . . To be continued . . . .") (last visited Oct. 18, 2023).

258 *New Trans-Atlantic Data Privacy Framework Largely a Copy of "Privacy Shield"*. Noyb *Will Challenge the Decision*, *supra* note 249; *see also* Alina Clasen, *New EU-US Data Transfer Deal Also Faces Criticism in Germany*, EURACTIV (Sept. 14, 2023), https://www.euractiv.com/section/data-protection/news/new-eu-us-data-transfer-deal-also-faces-criticism-in-germany [https://perma.cc/TUT9-YWQE] ("It is highly likely that Schrems will file a suit with an Austrian court in the autumn, which will then refer the case to the EU Court of Justice for a preliminary ruling. To file a case in Austria, Schrems will first have to wait for 10 October, when US companies registered in the commercial register and listed in the data protection framework will be able to exchange data with the EU.").

259 *New Trans-Atlantic Data Privacy Framework Largely a Copy of "Privacy Shield"*. Noyb *Will Challenge the Decision*, *supra* note 249.

260 *See* Press Release, Philippe Latombe, Député de la Vendée, Communiqué de Presse (Sept. 21, 2023), https://twitter.com/platombe/status/1704901010404061231/photo/1 (last visited Oct. 6, 2023) (stating that "[n]os analyses convergent, nos actions sont complémentaires," or "[o]ur

### B. *The New Redress Mechanism*

The new redress mechanism to review qualifying complaints created by EO 14086, including its accompanying AG Regulation establishing the DPRC, is a considerable improvement compared to the previous ombudsperson mechanism of the invalidated Privacy Shield Decision.[261] As discussed in Section III.B.2 of this Article, the new redress mechanism consists of two layers: (1) the CLPO's initial investigation of qualifying complaints, and (2) the DPRC and its review of CLPO's determinations upon receipt of an application from the complainant or an IC element.[262]

In particular, EO 14086 introduces several safeguards with respect to the DPRC. As mentioned, the DPRC judges "shall not be, at the time of their initial appointment, employees of the United States Government" and "[d]uring their term of appointment on the Data Protection Review Court, such judges shall not have any official duties or employment within the United States Government other than their official duties and employment as judges on the Data Protection Review Court."[263] In addition, the Attorney General who appoints the DPRC judges "shall not interfere with a review by a Data Protection Review Court panel of a determination the CLPO made regarding a qualifying complaint."[264] The Attorney General shall also usually not "remove any judges appointed . . . , or remove any judge from service on a Data Protection Review Court panel."[265]

As discussed, the DPRC panel of three judges will also select a special advocate who will especially advocate concerning the complainant's interest in the matter.[266] Moreover, the CLPO's determinations shall be "impartially review[ed]" by the DPRC panel concerning "whether a covered violation occurred and the appropriate remediation in the event there was such a violation."[267] The DPRC panel also has the power to adopt decisions that are binding.[268] The CJEU particularly pointed out

---

analyses converge, our actions are complementary" (unofficial translation from French to English)).

261 For more information on the ombudsperson mechanism, see *supra* Section I.B. For more information on the new redress mechanism and the DPRC, see *supra* Section III.B.2.

262 Exec. Order 14086 § 3(c)–(d), 87 Fed. Reg. at 62290–93.

263 *Id.* § 3(d)(i)(A), 87 Fed. Reg. at 62291. For more information, see *supra* Section III.B.2.

264 *Id.* § 3(d)(iv), 87 Fed. Reg. at 62292. For more information on the appointment of judges, see 28 C.F.R. § 201.3 (2023).

265 Exec. Order 14086 § 3(d)(iv), 87 Fed. Reg. at 62292.

266 *Id.* § 3(d)(i)(C), 87 Fed. Reg. at 62291. For more information on special advocates, see 28 C.F.R. §§ 201.4, 201.8 (2023); *see also supra* Section III.B.2.

267 Exec. Order 14086 § 3(d)(i)(D), 87 Fed. Reg. at 62291. For more information on the DPRC panel's review, see 28 C.F.R. § 201.9 (2023).

268 Exec. Order 14086 § 3(d)(ii), 87 Fed. Reg. at 62292; 28 C.F.R. § 201.9(g).

this deficiency in the previous ombudsperson mechanism in *Schrems II*,[269] so this is a significant improvement. Furthermore, the PCLOB agreed to conduct annual reviews of the redress process.[270]

Again, despite these safeguards introduced with EO 14086, including its accompanying AG Regulation, there are three main concerns with the new redress mechanism that may likely lead the CJEU to conclude in a possible *Schrems III* case that the United States fails to offer data subjects guarantees essentially equivalent to those required by Article 47 (right to effective judicial protection) under the Charter.

First, the biggest issue is that the DPRC belongs to the executive branch instead of the judiciary.[271] It is *not* unlikely that the CJEU would conclude, similarly as in *Schrems II*,[272] that the DPRC's independence from the executive is undermined. Even though EO 14086 introduces safeguards that shall ensure the independence of DPRC judges, they likely do not go far enough. The problem is that even if the Attorney General cannot interfere with a DPRC's panel review and usually cannot remove DPRC judges from service on a panel, the U.S. President still can.[273] Schrems has also already expressed concerns, stating that "it is clear that this 'court' is simply not a court."[274]

Second, there is also no independence required for the special advocate who will advocate concerning the complainant's interest in the matter.[275] The safeguard that the special advocates "at the time of their initial appointment have not been employees of the executive branch in the previous two years" may not be sufficient.[276]

Third, another issue is that after completion of the review, the DPRC will only "inform the complainant . . . that 'the review either did not

---

269 *Schrems II*, ECLI:EU:C:2019:1145, ¶ 196; *see supra* Section I.B.

270 Exec. Order 14086 § 3(e)(i), 87 Fed. Reg. at 62293; Press Release, Priv. and C.L. Oversight Bd., *supra* note 176.

271 Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 9; *see also* Andrej Savin, *The New Framework for Transatlantic Data Transfers* 7, 12 (Copenhagen Bus. Sch. Law Rsch. Paper Series, Paper No. 23-01, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4494289 [https://perma.cc/L9BR-G3ZX]. For a contrary opinion, see, e.g., Théodore Christakis, Kenneth Propp & Peter Swire, *The Redress Mechanism in the Privacy Shield Successor: On the Independence and Effective Powers of the DPRC*, IAPP (Oct. 11, 2022), https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc [https://perma.cc/H4AH-FBNT].

272 *Schrems II*, ECLI:EU:C:2019:1145, ¶¶ 190, 195; *see also supra* Section I.B.

273 Exec. Order No. 14086 § 3(d)(iv), 87 Fed. Reg. 62292; *see also* Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 9. The EDPB also asked for clarification. *See European Data Protection Board Opinion 5/2023*, *supra* note 196, ¶ 225.

274 *New US Executive Order Unlikely to Satisfy EU Law*, *supra* note 242.

275 Exec. Order No. 14086 § 3(d)(i)(C), 87 Fed. Reg. 62291. *See also* Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 9.

276 28 C.F.R. § 201.4(a) (2023).

identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation.'"[277] In other words, the DPRC's decisions are classified and not made available to complainants.[278] This is problematic because the CJEU has already highlighted in *Schrems I* that

> legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.[279]

However, without access to the DPRC's decision, the complainant has no chance to exercise these rights.[280] The problem is compounded even more by the fact that the decisions of the DPRC are final and there is no way for complainants to appeal the court's decision in a federal court.[281]

Consequently, the CJEU may invalidate Privacy Shield 2.0 in a possible *Schrems III* case on the grounds that the United States fails to ensure an adequate level of protection under Article 45 of the GDPR, read not only in light of Articles 7 and 8 of the Charter, as established above,[282] but also in light of Article 47 of the Charter. The EC should have refrained from adopting Privacy Shield 2.0 and instead continued negotiations with the United States to address the identified shortcomings. After all the yearslong efforts the U.S. government and the EC have put toward a new Trans-Atlantic Data Privacy Framework, it is a pity to see that Privacy Shield 2.0 was adopted in its current version without addressing the identified concerns to guarantee a robust framework that has a chance to stand its ground before the CJEU. As the European Parliament has already correctly pointed out, the EC should "act in the interest of EU businesses and citizens by ensuring that the proposed framework

---

277 Exec. Order No. 14086 § 3(d)(i)(H), 87 Fed. Reg. 62292.

278 Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 8.

279 *Schrems I*, ECLI:EU:C:2015:650, ¶ 95. For more information, see *supra* Sections I.A, I.C.

280 *See also* Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 8. The EDPB also expressed concerns about the limited information given to complainants. *See European Data Protection Board Opinion 5/2023*, *supra* note 196, at 5.

281 28 C.F.R. § 201.9(g) (2023); *see also* Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 8; *European Data Protection Board Opinion 5/2023*, *supra* note 196, at 5.

282 *See supra* Section IV.A.

provides a solid, sufficient and future-oriented legal basis for EU-US data transfers."[283]

### C. *U.S. Federal Privacy Law*

Despite the current presence of an adequacy decision, the United States would be well advised to enact a comprehensive federal privacy law. Adopting such a law is not necessarily a precondition for addressing the shortcomings the CJEU underlined in *Schrems I* and *Schrems II*, but it still has benefits compared to the current U.S. approach.

First, a comprehensive federal privacy law that supersedes state privacy laws would create a harmonized approach to data protection in the United States. California, Virginia, Colorado, Utah, Connecticut, Iowa, Indiana, Tennessee, Montana, Texas, Oregon, and Delaware have all recently passed comprehensive privacy laws that are highly inspired by the EU GDPR, give consumers rights over their data, and impose obligations on businesses.[284] More states are expected to pass new privacy laws in the future,[285] which are certainly steps in the right direction. The issue, however, is that while the new state privacy laws are similar, they also differ from one another, making it difficult for businesses to keep track of and comply with them. A new comprehensive federal privacy law would eliminate the current labyrinth of privacy laws at the state level and help companies to better comply with U.S. law.[286] In addition, the privacy of all data subjects in the United States would be adequately protected, not just those residing in the aforementioned states that have passed new comprehensive privacy laws.[287]

Second, a new U.S. federal privacy law would certainly also help to demonstrate the satisfaction of Article 45 of the GDPR and an essentially equivalent level of data protection to what is guaranteed in the EU. Thus, such a law could promote cross-border transfers of personal data between the EU and the U.S. and transatlantic trade.[288] The European Parliament

---

283 Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 20.

284 *US State Privacy Legislation Tracker, Comprehensive Consumer Privacy Bills*, IAPP (Oct. 20, 2023), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/PMR2-FE9Y].

285 *Id.*

286 In the context of artificial intelligence/machine learning health apps, *see* Sara Gerke & Delaram Rezaeikhonakdar, *Privacy Aspects of Direct-to-Consumer Artificial Intelligence/Machine Learning Health Apps*, 6 INTELLIGENCE-BASED MEDICINE 100061 (2022), https://www.sciencedirect.com/science/article/pii/S266652122200014X?via%3Dihub.

287 *Id.* at 3–4.

288 *Id.* at 2, 4.

has also pointed out in its resolution from May 2023 that, compared to all other countries for which the EC has adopted adequacy decisions, the United States is the only country that has no federal privacy law.[289] The issue with the current approach of EO 14086 is that the U.S. President can change or repeal it at any time without the need to ask Congress or inform the EU.[290] The U.S. President could even issue secret Executive Orders.[291] Privacy Shield 2.0 can only be considered a "partial" adequacy decision in the absence of a U.S. federal privacy law. Only those organizations in the United States that self-certify to the U.S. Department of Commerce and are included in the Data Privacy Framework List benefit from easier transfers of personal data without the need for additional data protection safeguards.[292]

## CONCLUSION

The cross-border transfer of personal data is a crucial part of the EU-U.S. business relationship. This Article is the first to thoroughly analyze Privacy Shield 2.0, adopted by the EC on July 10, 2023, in order to restore transatlantic data flows and commercial exchanges between the EU and the United States. The failure of the United States to recognize the privacy rights of EU data subjects has already given rise to two groundbreaking cases before the CJEU in 2015 and 2020, namely *Schrems I* and *Schrems II*. Part I has discussed both of these cases and carved out the main reasons for the CJEU to invalidate the Safe Harbor Decision in *Schrems I* and the Privacy Shield Decision in *Schrems II*. It has also compared both cases and drawn lessons learned from them. In particular, it has shown that neither the Safe Harbor Decision nor the Privacy Shield Decision limited interference with fundamental rights to what is strictly necessary. In addition, both decisions did not provide data subjects with the right to effective judicial protection.

Part II has analyzed the practical implications of the invalidation of the Privacy Shield Decision in *Schrems II*. In particular, it has shown that the CJEU's judgment has led to considerable uncertainties and difficulties in transferring personal data from the EU to a third country. In the past

---

289 Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 12. For the countries for which the EC has adopted adequacy decisions, see *supra* Introduction.

290 Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework, *supra* note 210, ¶ 12.

291 *Id.*

292 *See* European Commission Factsheet MEMO/17/15, *supra* note 26; European Commission Press Release IP/23/3721, *supra* note 18. For more information, see *supra* Section III.D.4.

almost three years, in the absence of a valid adequacy decision, companies and other bodies had to rely on different mechanisms, especially SCCs, for cross-border transfers of personal data from the EU to the United States. However, Part II has carved out the issue that although the CJEU upheld the validity of the SCC Decision, the court highlighted the need for "supplementary measures" to compensate for any lack of data protection without further discussing what such measures could look like. To highlight these legal uncertainties for companies and other bodies, Part II has also explored the Irish DPC's recent decision from May 2023 regarding Meta Platforms Ireland Limited, which resulted in a record €1.2 billion fine for infringing Article 46(1) of the GDPR.

Part III has discussed in-depth four relevant events toward the adoption of Privacy Shield 2.0: (1) the announcement of a new Trans-Atlantic Data Privacy Framework, (2) the release of EO 14086, (3) the EC's draft adequacy decision, (4) the launch of the adoption process and the ultimate adoption of the adequacy decision. For example, Part III has thoroughly analyzed the new safeguards for U.S. signals intelligence activities and the new signals intelligence redress mechanism introduced by sections 2 and 3 of EO 14086. Understanding these changes is especially important to assess whether the concerns expressed by the CJEU in *Schrems I* and *Schrems II* have been satisfactorily addressed. Part III has also elaborated on the adoption process of Privacy Shield 2.0. In particular, it has examined the recent opinions from the European Parliament and the EDPB, both of which expressed doubts as to whether the improvements in EO 14086 are sufficient to address the CJEU's concerns. Despite these opinions, the EC received the green light by twenty-four votes in favor and three abstentions from the committee comprised of representatives of the EU Member States, and the EC went ahead and adopted Privacy Shield 2.0 on July 10, 2023.

Lastly, Part IV has discussed the content of EO 14086 further and analyzed whether the United States successfully addressed the CJEU's concerns in *Schrems I* and *Schrems II*, and thus has an essentially equivalent level of data protection to what is guaranteed in the EU. It argued that it is *not* unlikely that the CJEU would invalidate Privacy Shield 2.0 in a possible *Schrems III* case on the grounds that the United States fails to ensure an adequate level of protection under Article 45 of the GDPR, read in light of Articles 7, 8, and 47 of the Charter.

Part IV has demonstrated that there is no harmonized understanding of the meaning of the terms "necessary" and "proportionate" in the United States and EU. Moreover, the permissibility of bulk collection of signals intelligence is not dependent on an independent authority's prior authorization, and the U.S. President

has complete discretion on whether to add objectives for which signals intelligence collection activities or bulk collection may be used.

Part IV has also argued that although the new redress mechanism to review qualifying complaints created by EO 14086, including its accompanying AG Regulation establishing the DPRC, is a considerable improvement compared to the previous ombudsperson mechanism, this safeguard is likely also insufficient to address the CJEU's concerns. In particular, the DPRC belongs to the executive branch instead of the judiciary, and the CJEU may likely conclude in a possible *Schrems III* case that the DPRC's independence from the executive is undermined. In addition, there is no independence required for special advocates, and the DPRC's decisions are classified and not made available to complainants.

Consequently, this Article concludes that the EC should have refrained from adopting Privacy Shield 2.0 and instead continued negotiations with the United States to address the identified shortcomings. In the interests of businesses and individuals, the adequacy decision should only have been adopted if it had been solid enough to likely stand its ground before the CJEU in a possible *Schrems III*. Unfortunately, this is not the case with Privacy Shield 2.0. In the long run, the United States would also benefit from a comprehensive federal privacy law that ensures adequate protection of personal data for all data subjects in the United States. Such a law could not only eliminate the current clutter of privacy laws at the state level but also support a claim that the United States has an essentially equivalent level of data protection to what is guaranteed in the EU.

## ACKNOWLEDGMENT

This work was funded by the European Union (Grant Agreement no. 101057321). Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them. S.G. also reports grants from the European Union (Grant Agreement no. 101057099), the National Institute of Biomedical Imaging and Bioengineering (NIBIB) and the National Institutes of Health Office of the Director (NIH OD) (Grant Agreement no. 3R01EB027650-03S1 and no. 1R21EB035474-01), and the National Institute on Drug Abuse (NIDA)/National Institutes of Health (NIH) (Grant Agreement no. 1U54DA058271-01).