InDret
3.2025

# Transnational Data Transfers under GDPR: a Look Insight the Latest Agreement with the United States

Briseida Sofía Jiménez-Gómez
Universidad Complutense de Madrid
-

***Abstract***

**-**

*Processing of personal data of European Union citizens and residents by U.S. companies has been marked by constant challenges. A noteworthy development was the publication of an adequacy decision by the European Commission on 10 July 2023 with respect to personal data transfers from the European Union to the United States. This new agreement is named the EU-US Data Privacy Framework, which in principle responds to the legal concerns raised by the Court of Justice of the European Union in the landmark case Schrems II, that invalidated the Privacy Shield decision. This paper addresses the legal risks for data transfers from the European Union to the United States, considering the new agreement between the EU Commission and the United States. It is crucial to assess whether this data privacy framework involves a paradigm shift with regard to the EU citizens and residents' rights since the most prominent technology companies operating in the European Union are based in the United States. The first periodic review carried out by the EU Commission (9 October 2024) and the European Data Protection Board Report on the first review (4 November 2024) are included in the analysis to demonstrate the shortcomings of the EU-U.S. Data Privacy Framework.*

**Sumario**

**-**

*El tratamiento de datos personales de ciudadanos y residentes de la Unión Europea por parte de empresas estadounidenses ha estado marcado por constantes desafíos. Un avance notable fue la publicación de una decisión de adecuación por parte de la Comisión Europea el 10 de julio de 2023 con respecto a las transferencias de datos personales de la Unión Europea a los Estados Unidos. El nuevo acuerdo se denomina Marco de Privacidad de Datos UE-EE. UU. y, en principio, responde a las preocupaciones jurídicas planteadas por el Tribunal de Justicia de la Unión Europea en el famoso caso Schrems II, que anuló la decisión de adecuación previa (el Escudo de privacidad). Este artículo aborda los riesgos jurídicos de las transferencias de datos de la Unión Europea a los Estados Unidos, teniendo en cuenta el nuevo acuerdo entre la Comisión Europea y los Estados Unidos. Resulta fundamental evaluar si el nuevo marco de protección de datos consiste en un cambio de paradigma para el respeto de los derechos de los ciudadanos y residentes de la Unión Europea, ya que las empresas tecnológicas más importantes que operan en la Unión Europea tienen su sede en los Estados Unidos. Se incluyen en el análisis tanto el informe de la primera revisión periódica llevada a cabo por la Comisión de la UE (9 de octubre de 2024) como el informe del Comité Europeo de Protección de Datos sobre la primera revisión (4 de noviembre de 2024) para demostrar las deficiencias del Marco de Privacidad de Datos UE-EE.UU.*

***Título:*** Transferencias transnacionales de datos bajo el RGPD: una mirada al último acuerdo con Estados Unidos

**-**

***Keywords*****:** *EU-U.S. Data Privacy Framework, surveillance, privacy, data protection, fundamental rights, adequacy decision*

**Palabras clave:** *Marco de Privacidad UE-EE.UU, vigilancia, intimidad, protección de datos, derechos fundamentales, decisión de adecuación*
**-**
**DOI:** 10.31009/InDret.2025.i3.17

InDret

3.2025

Recepción
30/07/2024
-
Aceptación
13/05/2025
-

## Índice

-



-

# 1. Context*

## 1.1. Introduction

The harmonization process within the EU relied on the free flow of personal data to foster growth. Directive 45/95/EC[1] was the first step in the European Union to harmonize personal data protection, and it implied that the level of protection of personal data increased because many of the EU Member States did not previously have a data protection regime. Therefore, data flows cannot be an impediment within the EU because one of the main economic objectives was creating a market Union.

The General Data Protection Regulation (EU) 2016/679[2] implied a step further in the harmonization process, creating a directly applicable instrument in every Member State. The Directive idea continues with the GDPR, which is enhancing a uniform and high level of protection of natural persons and eliminating obstacles to circulation of personal data within the Union. The GDPR establishes free circulation of personal data within the geographical space of the EU (and the EEA)[3]. However, as the GDPR does not need a transposition on national legislation, if a EU controller transfers personal data to a processor in a non-EU country, EU law applies directly to data controllers and data processors[4]. It was suggested that that data flows should be the fifth freedom of the internal market[5]. In this way, the Regulation EU 2018/1807 enhances the principle of free flow of data within the EU/EEA territory with regard to non-personal data[6].

---

* Part of this paper was presented at the Luxembourg Centre of European Law of the University of Luxembourg on 22 July 2024 during my visiting research period. ORCID 0000-0003-0862-8188, Profesora Titular (ac) de Derecho Mercantil, Universidad Complutense de Madrid. ICEI Member. LL.M. College of Europe, Postdoctorate Harvard Law School. This work has been carried out within the framework of the national Spanish research project PID2023-147982OB-I00, «Simplificación y digitalización de los procesos de movilidad y reestructuración societaria». I would like to thank the external reviewers of *Indret* for their comments, which I have incorporated into the final version. All websites have been last visited on 13.05.2025.

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

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[3] General Data Protection Regulation, Art. 1(3).

[4] *See* Moerel, Lokke, *Binding Corporate Rules*, Corporate Self-Regulation of Global Data Transfers, Oxford University Press, 2012, pp. 46-47, discussing some differences between the Directive and the GDPR.

[5] *See*, Press release, *Free flow of non-personal data: Parliament approves EU's fifth freedom*, 4.10.2018, available at https://www.europarl.europa.eu/news/en/press-room/20180926IPR14403/free-flow-of-non-personal-data-parliament-approves-eu-s-fifth-freedom; AKKERMANS, Bram, «The Influence of the Four (or Five) Freedoms on Property Law», in VAN ERP, Sjef and ZIMMERMANN, Katja (eds.), *Research Handbook on European Union Property Law,* Northampton, Edward Elgar Publishers, 2023 , SSRN version, p. 7, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4232332

[6] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), PE/53/2018/REV/1, *OJ L 303, 28.11.2018*.

The GDPR model has been successful internationally, specifically the GDPR crosses European borders when third states decide to regulate personal data protection using EU law as a model[7]. Moreover, the data controller cannot choose which set of rules is applicable as this is a consequence on an inelastic market dominated by the «Brussels Effect»[8]. However, the GDPR model is within the framework of a specific international organization with a common political interest. Data protection means not only limiting access to personal information, so that citizens maintain the right to the information they want to show about themselves, but data protection is concerned with ensuring that data flows properly within the EU and abroad[9]. On the one hand, very high data protection can excessively restrict economic activities and trade[10]. On the other hand, lack of data protection or very weak protection can create negative effects in the market that affect consumer confidence. That is why the material scope of the GDPR is vast, including processing of personal data wholly or partly by automated means, and processing of personal data which form part of a filing system or are intended to form part of a filing system[11].

Besides, personal data located on EU territory seems to dictate control, because the GDPR restricts transfer of data outside the EU if appropriate safeguards are not in place[12]. The GDPR expands its territorial scope beyond the EU under the idea that data protection is a fundamental right that must continue, regardless of where personal data is processed. Indeed, legal protection follows the data that has been included under the principle of personality[13]. One of the objectives of regulating cross-border data flows is to promote social and economic values[14]. Despite this, the EU Charter of Fundamental Rights does not mention the regulation of cross-border data flows, but rather refers to the «essence» of fundamental rights and freedoms[15]. The Court of Justice of the European Union has confirmed that the high level of protection of natural persons guaranteed by the GDPR is not undermined abroad, especially the protection of personal data relating to natural persons who are citizens or residents in the EU, in accordance with article 44 of the GDPR, and the EU Charter of Fundamental Rights [16].

---

[7] GREENLEAF, Graham, « 'European' Data Privacy Standards Implemented in Laws Outside Europe», *Privacy Laws and Business International Report*, 2017, vol. 149, no. 1, pp. 21-23, UNSW Law Research Paper No. 18-2, available at SSRN: https://ssrn.com/abstract=3096314.

[8] Bradford, Anu, The Brussels Effect: How the European Union Rules de World, Oxford University Press, 2020, p. 142.

[9] NISSENBAUM, Helen, *Privacy in Context: Technology, Policy, and The Integrity of Social Life*, Stanford University Press, 2010, pp. 2-3.

[10] *See* CHANDER, Anupam, SCHWARTZ, Paul M., «Privacy and/or Trade», *University Chicago Law Review*, vol. 90, issue 1, 2023, pp. 49-135, p. 70: «Bracketing privacy allowed regulatory space for a country to provide privacy protections, but only if these safeguards did not unduly interfere with trade».

[11] *See* GDPR, article 2 (1).

[12] *See* GDPR, article 46.

[13] *See* KUNER, Cristopher, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013, p. 123.

[14] *See Ibid.*, p. 160.

[15] *See* Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389, art. 52.

[16] Case C-362/14 Maximilien Schrems v. Data Protection Commissioner [2015] EU:C:2015:650 [hereinafter Schrems I]; Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd, Maximilien Schrems [2020] EU:C:2020:559 [hereinafter Schrems II]. See also CJEU, Opinion 1/15, Draft Agreement Between Canada and the European Union, (26.07. 2017) EU:C:2017:592 (invalidating the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data).

Similar restrictions for personal data are applied to EU institutions, bodies and agencies under Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 (hereinafter Regulation 2018/1725)[17].

In an international context different terminology on the subject takes us into the difference between legal systems that are not European or that do not have legislation inspired by the General Data Protection Regulation and European laws. United States is one of the paradigmatic examples that has a different regulation to the European Union. Sometimes, even in legal documents, the problem of terminology arises. For example, in the latest adequacy decision of the European Commission the term «privacidad de datos» is used to translate «data privacy». However, neither under Spanish Law nor under European Law does «privacidad de datos» exist. Data protection is the correct terminology under EU law, and data protection can be included within the fundamental right of privacy. However, data protection has also been considered a fundamental right by itself. With respect to data protection beyond the European Union and to the United States, it should be noted that there are two approaches to cross-border data flows. In recent decades, the discourse has been that the United States offers a market-dominated approach, while the EU was immersed in a more protectionist policy of citizens[18]. Certain advances can be observed within U.S. data protection law, and mutual regulatory influences are even recognized, at least at the level of substantive law[19].

This article is divided into four parts. Part 1 discusses the finding of the CJEU in two landmark cases, Schrems I[20] and Schrems II[21]. The CJEU invalidated the EU Commission adequacy Decision in force until the judgment that permitted to transfer safely personal data from the European Union to the United States in two ocassions. The grounds that the CJEU claimed are still relevant to foresee the limits to transfer personal data from the European Union to the United States under Chapter V of the GDPR, given that Schrems announced its intention to pursue legal actions against the current adequacy Decision 2023/1795 under the EU-U.S. Data Privacy Framework (DPF) [22].

Part 2 provides some legal mechanisms to transfer personal data beyond the EU like standard contractual clauses, binding corporate rules and specific derogations. These alternative mechanisms have been used for many companies in the interim period between the invalidation

[17] Arts. 46-51 of the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text With EEA Relevance.) PE/31/2018/REV/1, OJ L 295, 21.11.2018.

[18] REIDENBERG, Joel R., «Resolving Conflicting International Data Privacy Rules in Cyberspace», *Stan. L. Rev*., vol. 52, 1999-2000, p. 1315 y ss., p. 1318.

[19] JIMÉNEZ-GÓMEZ, Briseida Sofía, «Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute», *Santa Clara Journal of International Law*, vol. 19, issue 2, 2021, pp. 1-45, pp. 8-9.

[20] Case C-362/14 Maximilien Schrems v. Data Protection Commissioner [2015] EU:C:2015:650 [hereinafter Schrems I]. 6.10.2015.

[21] Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd, Maximilien Schrems [2020] EU:C:2020:559 [hereinafter Schrems II]. 16.07.2020.

[22] Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Brussels, 10.7.2023 C(2023) 4745 final https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

of the Privacy Shield Decision[23] and the Data Privacy Framework Decision. Despite being an alternative mechanism, some limitations are currently present with these tools in the light of interpretation of the Schrems II case, recent national decisions on Uber and Microsoft and a new Judgment of the General Court[24]. Part 2 also sets out a preliminary critique on the EU-U.S. Data Privacy Framework adopted by the EU Commission on 10 July 2023 as the adecuacy Decision 2023/1795.

Part 3 examines several issues on the adecuacy Decision 2023/1795, from formality to the new Executive Order 14086 on Safeguards for U.S. Signals Intelligence Activities established in the United States as a reaction to the Schrems II case, including the difference terminology between the EU and the U.S. It analyses the two layer mechanism to address the right to an effective remedy under article 47 of the EU Charter of Fundamental Rights. The Data Protection Review Court and the Civil Liberties Protection Officer should be an effective remedy for EU data subjects under surveillance. In addition, this part also evaluates the redress options in complaint handling. Furthermore, it explores the developments in the U.S. legal system since several state privacy laws are emerging in the U.S., some of them including safeguards on automated processing. However, it also navigates the challenges and difficulties under U.S. law to be of equivalent protection under article 45 of the GDPR read in light of articles 7, 8 and 47 of the EU Charter. It discusses some legal difficulties such as the lack of a general federal privacy law, limited standing before the U.S. Supreme Court, which together with claims of government secrecy prevents citizens from obtaining effective remedies for privacy violations.

Part 4 discusses the EU institutions perspectives towards the Privacy Data Framework. The first section explores the situation before passing the adequacy Decision during the launch of its adoption process, where the European Parliament and the European Data Protection Board expressed its opinion. The second section analyses the answer of the European Commission (9 October 2024) and the European Data Protection Board (4 November 2024) on the first review of the adequacy Decision.

Part 5 concludes that the Data Privacy Framework is an improvement in comparison to the past situation (the Ombudsman mechanism, the more targeted objectives by Signal activities), but not robust enough to pass the examination of the Court of Justice of the European Union. The disadvantage is transatlantic data flows remain an unestable area with potential future impact in companies operating cross-border.

### 1.2. The Court of Justice judgment on Schrems I

#### *a. Start*

The effects of Snowden's revelations to the media brought the issue to a judicial level following the filing of a complaint against Facebook Ireland, a subsidiary of Facebook Inc. (the latter based in the U.S. now Meta), by Mr. Schrems, an Austrian citizen and user of the social network Facebook on 25 June 2013, in which he requested the cessation of the transfer of his personal

[23] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance), C/2016/4176, *OJ L 207, 1.8.2016.*
[24] T-354/22 Bindl v Commission [2025] (ECLI:EU:T:2025:4) 8.01.2025.

data to the U.S.[25] First, the Irish supervisory authority refused to investigate the complaint made by Mr. Schrems on the grounds that it was unfounded, it was turned into an appeal before the Irish High Court and this court admitted it and refers to the CJEU. The Irish High Court considered that mass and undifferentiated accessing of personal data infringes the Irish Constitution and that the Commissioner was wrong in rejecting the complaint, given the existence of a serious doubt as to whether the United States ensures an adequate level of protection of personal data, at least on the basis of Irish law alone[26]. Although the applicant had not formally challenged its validity, he was in fact challenging the lawfulness of the Safe Harbour regime established in Decision 2000/520/EC[27].

However, this case was related to the interpretation of EU law, in particular, whether Decision 2000/520 does satisfy the requirements arising from both Articles 7 and 8 of the EU Charter and from the principles enunciated by the Court of Justice in the *Digital Rights Ireland and Others* judgment[28]. According to the High Court, Decision 2000/520 does not satisfy these requirements[29]. Therefore, the Irish High Court submitted two preliminary questions to the CJEU as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to release himself, where appropriate, from such a finding[30].

*b. Essentially equivalent protection*

Schrems I constitutes the first CJEU ruling addressing the analysis of international data transfers in accordance with EU Treaties and the EU Charter of Fundamental Rights. Following the opinion of Advocate General Y. Bot, the CJEU specifies for the first time, with regard to international transfers of personal data, the concept of adequate level of protection as a formula that requires that the third country «in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter»[31]. Otherwise, the high level of EU protection would be easily circumvented by transferring personal data to third countries for the purpose of being processed in those countries. Nothwithstanding, «the word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order»[32]. The means for ensuring a high level of protection must nevertheless prove, in practice, «effective in order to ensure protection essentially equivalent to that guaranteed within the European Union»[33]. And, as the level of protection in a third country

[25] Case C-362/14 Maximilien Schrems v. Data Protection Commissioner [6.10.2015] (ECLI:EU:C:2015:650) [hereinafter Schrems I].
[26] Schrems I, para. 33.
[27] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), *OJ L 215, 25/08/2000*.
[28] Joined Cases C-293/12 and C-594/12, [6.10.2015] (ECLI:EU:C:2014:238).
[29] Schrems I, para. 34.
[30] Schrems I, para. 76.
[31] Schrems I, para. 73.
[32] *Ibid.*
[33] Schrems I, para. 74.

may evolve, it is up to the European Commission to verify regularly whether the level of protection in the country in question remains adequate[34]. Moreover, the level of protection ensured by the third country in question must be factually and legally justified, but «such a check is required, in any event, when evidence gives rise to a doubt in that regard».[35]

The CJEU substantiates its ruling on two essential aspects that are decisive for declaring, in the final instance, the invalidity of Decision 2000/520/EC.

First, the Safe Harbour principles[36] 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.»[37]

Second, 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.[38]» In this regard, it considers that the European Union Decision grants priority to the requirements of national security, public interest and compliance with U.S. law over the Safe Harbour principles, thereby incorporating a general derogation that allows for «interference» with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States [39].

Recalling the shortcomings identified by the Commission to which reference has been made previously, the CJEU held that , «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»[40].

The CJUE noted that «legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail»[41].

[34] Schrems I, para. 76.
[35] Schrems I, para. 76.
[36] For a description and advantages of the Safe Harbour Principles *see* Ortega Giménez, Alfonso, «¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EE.UU.», *Cuadernos de Derecho Transnacional*, 2024, Vol. 16, Nº 1, 2024, pp. 483-513, pp. 484-485. On the problems, *see* Jiménez-Gómez, Briseida Sofía, «Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute», *Santa Clara Journal of International Law*, vol. 19, issue 2, 2021, pp. 1-45, pp. 16-18.
[37] Schrems I, para. 82.
[38] Schrems I, para. 86.
[39] Schrems I, para. 87.
[40] Schrems I, para. 94.
[41] Schrems I, para. 93.

Moreover, the CJUE found 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»[42].

*c. Result: Safe Harbour invalidation*

Schrems I case concludes with the declaration of the invalidity as a whole of Decision 2000/520/EC and with it, of the Safe Harbor system for the transfer of personal data from the EU to the United States. In particular, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments[43].

### 1.3. The Court of Justice judgment on Schrems II

After the annulment of the adequacy decision (Safe Harbor), Facebook Ireland explained that the company was using the standard data protection clauses set out in the annex to the SCC Decision[44]. Schrems reformulated his complaint to the Data Protection Commissioner for investigation[45]. He claimed that, since that data was used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter, the SCC Decision cannot justify the transfer of that data to the United States. Therefore, Schrems asked the DPC to prohibit or suspend the transfer of his personal data to Facebook Inc[46]. The Irish Commissioner brought an action before the High Court, that referred questions for a preliminary ruling to the CJEU. Mr. Schrems' first complaint coincided in time with the negotiations between the European Commission and the U.S. authorities aimed at strengthening the Safe Harbor model, which, concluded with the adoption of a new instrument of legality for transfers of personal data between the EU and the U.S. called Privacy Shield[47].

The three main findings of the Schrems II case are the following: that the second adequacy decision called Privacy Shield is invalid, that standard contractual clauses under the Commission

[42] Schrems I, para. 95.
[43] Schrems I, para. 97.
[44] Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance), *OJ L 39, 12.2.2010*. This text is no longer in force. It was repealed by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), C/2021/3972, *OJ L 199, 07/06/2021*.
[45] Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd, Maximilien Schrems [16.07.2020] ECLI:EU:C:2020:559 [hereinafter Schrems II].
[45] Schrems II, para. 54.
[46] Schrems II, para. 55.
[47] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, C/2016/4176, *OJ L 207, 1.8.2016*.

Decision 2010/87/EU of February 2010 as such are valid alternative mechanisms[48], and that surveillance can only be legal if the United States offers an equivalent level of protection.

*a. Scope of the GDPR*

The CJEU included within the scope of the GDPR the possibility that the personal data transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing for the purposes of public security, defence and State security by the authorities of that third country[49]. The CJEU observed that having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 4(2) of the GDPR[50]. The transfer from Facebook Ireland to Facebook Inc is between two legal persons, excluded to benefit from the derogation of data processing by a natural person in the course of a purely personal or household activity.[51]

*b. Standard contractual clauses*

The CJEU was asked to specify which factors need to be taken into consideration for the purpose of determining whether that level of protection is ensured in the context of transfers required by Article 46(1) and Article 46(2)(c) of the GDPR in respect of a personal data transfer to a third country based on standard data protection clauses.

First, recalling point 117 of the Advocate General's Opinion, the CJEU held that the provisions of Chapter V of the GDPR are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country, in accordance with the objective set out in recital 6 thereof.[52]

Second, the CJEU ruled that «appropriate guarantees must be capable of ensuring that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially equivalent to that which is guaranteed within the European Union»[53]. The Court reasoned its ruling on recital 107 of the GDPR where in the absence of an adequacy decision, the transfer of personal data to that third country should be prohibited, unless the requirements relating to transfers subject to appropriate safeguards are fulfilled. The controller or processor must «compensate for the lack of data protection in a third country» in order to «ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union»[54]. Thus, the Court followed the Advocate

[48] *See* KUNER, Christopher, «Schrems II Re-Examined», *Verfassungsblog* (25.08.2020), https://verfassungsblog.de/schrems-ii-re-examined/ («the only time the Court has given a positive endorsement to any data transfer mechanism»)
[49] Schrems II, para. 86.
[50] Schrems II, para. 83.
[51] Schrems II, para. 85.
[52] Schrems II, para. 93.
[53] Schrems II, para. 96.
[54] Schrems II, para. 95.

General's Opinion that agrees with Schrems and the Data Protection Commissioner from Ireland[55].

Third, the Court held that the interpretation of EU law and examination of the legality of EU legislation must be undertaken in the light of the fundamental rights guaranteed by the Charter[56]. This means that the benchmark is the EU Charter of Fundamental Rights and not the European Convention of Human Rights (ECHR) because the EU has not acceded to the ECHR, so it does not constitute a legal instrument formally incorporated into EU law[57]. However, Article 52(3) of the Charter provides that the rights contained in the Charter which correspond to rights guaranteed by the ECHR shall have the same meaning and scope as those established by that Convention.

The CJEU observed that, although Article 46(2)(c) of the GDPR does not list the various factors which must be taken into consideration for the purposes of assessing the adequacy of the level of protection to be observed in such a transfer, Article 46(1) of the GDPR states that data subjects must be afforded appropriate safeguards, enforceable rights and effective legal remedies[58]. The CJEU stated that any access by the public authorities of that third country to the personal data transferred and the relevant aspects of the legal system of that third country must be assessed to determine the level of adequacy[59]. Critically, «the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation[60]». The ruling is that Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to SCC are afforded a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR, read in the light of the Charter[61].

The Irish Commissioner found that the standard data protection clauses in the annex to the SCC Decision are not capable of remedying that defect, since they confer only contractual rights on data subjects against the data exporter and importer, without, however, binding the United States authorities[62]. However, the CJEU did not conclude the same because it differentiates a Commission decision finding adequacy under article 45 GDPR and a Commission decision adopting standard data protection clauses under article 46 GDPR. Before adopting the SCC

[55] Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, Case C-311/18, para. 115. (ECLI:EU:C:2019:1145).
[56] Schrems II, para. 99.
[57] Schrems II, para. 98. In the future this situation may change, Press release, Major progress on the path to EU accession to the ECHR: Negotiations concluded at technical level in Strasbourg, Delegation of the Council of Europe in Strasbourg, 31.03.2023, https://www.eeas.europa.eu/delegations/council-europe/major-progress-path-eu-accession-echr-negotiations-concluded-technical-level-strasbourg_en?s=51
[58] Schrems II, para. 103.
[59] Schrems II, para. 104.
[60] Schrems II, para. 104.
[61] Schrems II, para. 105.
[62] Schrems II, para. 56.

Decision, the Commission may not assess the adequacy of the level of protection ensured by the third countries to which personal data could be transferred pursuant to such clauses[63].

According to the CJEU, «Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by that regulation is not undermined, it may prove necessary to supplement the guarantees contained in those standard data protection clauses»[64]. SCC may require, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection[65]. Therefore, it will depend on the prevailing position in a particular third country. The Court added that «where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned»[66]. And, the Court gave an example: «where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data»[67]. Thus, where there are conflicting rules in the EU and the third country. In this context the Court interpreted 'the applicable data protection law', under the SCC Decision[68], according to the definition set out in that Decision, 'the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established'. That legislation includes the provisions of the GDPR, read in the light of the Charter[69].

The SCC Decision confers on the controller established in the European Union the right to suspend the transfer of data and/or to terminate the contract[70]. However, this right is an obligation in the light of the requirements of Article 46(1) and (2)(c) of the GDPR, read in the light of Articles 7 and 8 of the Charter. If not, the controller fails to fulfill its obligations under the SCC Decision[71]. Yet, «operators' assessments of the necessity of such an obligation must, where relevant, take into account a finding that the level of protection ensured by the third country in a Commission adequacy decision, adopted under Article 45(3) of the GDPR, is appropriate»[72].

[63] Schrems II, para. 130.
[64] Schrems II, para. 132.
[65] Schrems II, para. 133.
[66] Schrems II, para. 135.
[67] *Ibid.*
[68] The Court refers to Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance), *OJ L 39, 12.2.2010*. This text is no longer in force. It was repealed by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), C/2021/3972, *OJ L 199, 07/06/2021*.
[69] Schrems II, para. 138.
[70] Schrems II, para. 140.
[71] *Ibid.*
[72] Schrems II, para. 141.

Moreover, the risk of divergent decisions by national data protection authorities is diminished with the possibility for them to refer to the European Data Protection Board (EDPB) for an opinion, which may adopt a binding decision, when a national data protection authority does not follow its opinion pursuant to Article 65(1)(c) of the GDPR[73]. Schrems II was criticized because it reduced all the Chapter V GDPR mechanisms into a single adecuacy test, considered unworkable in practice[74]. Schrems II undermined the use of «appropriate safeguards» under article 46 of the GDPR since the controller or processor has to compensate for the lack of data protection in a third country. According to the CJEU, supplementary measures rectify legal problems that undermine equivalency[75] but «a level of protection essentially equivalent to that which is guaranteed within the EU» can mean legal adequacy as under Article 45 of the GDPR. Consequently, no other mechanism can address the incompatibility between third country law or practice under the GDPR. SCC, binding corporate rules and certifications mechanisms are all contractual in nature, so they do not bind other governments.

*c. Result: Privacy Shield invalidation*

The Court held that the Privacy Shield decision cannot ensure a level of protection essentially equivalent to that arising from the Charter[76]. The invalidity of the Privacy Shield is based on the lack of safeguards in U.S. surveillance programs like PRISM and UPSTREAM. It is acknowledged that access to, and use of, personal data transferred from the European Union to the United States by U.S. public authorities is an interference with the right to privacy and the right to data protection enschrined in Articles 7 and 8 of the Charter.

Although Articles 7 and 8 of the Charter are not absolute rights[77], personal data must be processed «for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law» pursuant to article 8(2) of the Charter[78]. Article 52 of the Charter marks off the limits of fundamental rights. On the one hand, 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[79]. The concept of essence of rights stems from the constitutional traditions common to the Member States and it is understood as a general principle of EU law[80]. On the other hand, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet

[73] Schrems II, para. 147.

[74] CORRALES COMPAGNUCCI, Marcelo, FENWICK, Marc, ABOY, Mateo and MINSSEN, Timo, «Supplementary Measures and Appropriate Safeguards for International Transfers of Health Data After *Schrems* II», in CORRALES COMPAGNUCCI, M. et al. (eds), *The Law and Ethics of Data Sharing in Health Sciences, Perspectives in Law, Business and Innovation*, Springer, Singapor, 2024, pp. 151-171, p. 155.

[75] Schrems II, para.134. CORRALES COMPAGNUCCI, *et al.*, «Supplementary Measures and Appropriate…», *op.cit.*, p. 158.

[76] Schrems II, para. 181.

[77] Schrems II, para. 172.

[78] Schrems II, para. 173.

[79] *See* Lenaerts, Koen, «Limits on Limitations: The Essence of Fundamental Rights in the EU», *German Law Journal*, vol. 20, 2019, pp. 779–793, p. 781. The author considers that a measure that compromises the very essence of a fundamental right is automatically disproportionate. Therefore, he proposes that in order for the concept of essence to function in a constitutionally meaningful way, both EU and national courts should apply the «respect-for-the-essence test» before undertaking a proportionality assessment.

[80] *Ibid.*, p. 780.

objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned[81]. On the principle of proportionality, «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. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing»[82].

The Court's assessment is pragmatic, instead of ascertaining beforehand whether that third country has complied with conditions essentially equivalent to those laid down in the first sentence of Article 52(1) of the Charter, the Court started to examine whether the implementation of those surveillance programmes is subject to legal requirements[83].

The Court found that E.O. 12333 does not confer rights which are enforceable against the U.S. authorities in the courts either[84] and that PPD-28 does not grant data subjects actionable rights before the courts against the U.S. authorities [85]. The FISC does not cover the issue of whether «individuals are properly targeted to acquire foreign intelligence information»[86]. The proportionality test failed because 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-U.S. persons potentially targeted by those programmes[87]. Under Article 45(2)(a) of the GDPR, a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights[88].

Consequently, the Court held that that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the U.S. authorities, from which it follows that data subjects have no right to an effective remedy[89]. Since bulk collection is allowed, «access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data»[90]. Bulk collection means that the Intelligence Community cannot use an identifier associated with a specific target to focus the collection. Moreover, the Ombudsperson

[81] Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 139 and the case-law cited).
[82] Schrems II, para. 176.
[83] Schrems II, para. 178.
[84] Schrems II, para. 182.
[85] Schrems II, para. 181.
[86] Schrems II, para. 179. The FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI). *See* Recital 109 of the Privacy Shield Decision.
[87] Schrems II, para. 180.
[88] Schrems II, para. 181.
[89] Schrems II, para. 192.
[90] Schrems II, para. 183.

Mechanism was not an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data equivalent to an effective remedy before a tribunal under article 47 of the Charter. The reasons were that the Ombudsperson was appointed by the Secretary of State and was an integral part of the U.S. State Department[91]. There was nothing in the Privacy Shield Decision to indicate that the dismissal or revocation of the appointment of the Ombudsperson is accompanied by any particular guarantees. Thus, this situation undermines the Ombudsman's independence from the executive[92]. In addition, there was nothing in that Decision to indicate that the Ombudsperson had the power to adopt decisions that were binding on those intelligence services and did not mention any legal safeguards that would accompany that political commitment on which data subjects could rely[93].

The European Data Protection Supervisor highlighted that the CJEU confirmed in Schrems II the criticism of the Privacy Shield repeatedly expressed by the EDPS and the EDPB[94]. The EDPS considers that «the protection of personal data requires actionable rights for everyone, including before independent courts. It is more than a "European" fundamental right – it is a fundamental right widely recognised around the globe. Against this background, the EDPS trusts that the United States will deploy all possible efforts and means to move towards a comprehensive data protection and privacy legal framework, which genuinely meets the requirements for adequate safeguards reaffirmed by the Court»[95].

## 2. Mechanisms to transfer personal data beyond the EU

### 2.1. The GDPR framework

A variety of mechanisms for transnational personal data transfers to third States are established to guarantee such a high level of protection of personal data under the articles 44 to 50 of the GDPR. The safest mechanism is that the third State or territory has an adequacy decision in place[96]. The GDPR provides that the adequacy decision can relate to a territory or a processing

[91] Schrems II, para. 195.
[92] *Ibid.*
[93] Schrems II, para. 196.
[94] *See* EUROPEAN DATA PROTECTION SUPERVISOR, EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II"), 17.07.2020, https://www.edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling_en
[95] *Ibid.*
[96] *See* GDPR, art. 45. The Commission concludes that each of the eleven countries and territories Andorra, Argentina, Canada (for commercial operators), Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay continues to ensure an adequate level of protection for personal data transferred from the European Union within the meaning of the GDPR, as interpreted by the Court of Justice. *Vid.*, Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, COM/2024/7 final, Brussels, 15.1.2024. Other countries with an adequacy decision are: Japan (2019), Republic of Korea (2021), United Kingdom (2021) and U.S.A. (2023). United Kingdom has two adequate decisions, one for transfers under the EU GDPR; and another for transfers under the Law Enforcement Directive. On 18 March 2025 the EU Commission published a Draft technical extension UK adequacy GDPR and a Draft technical extension UK adequacy LED to extend data flows with the UK for a period of six months, so they would be maintained until 27 December 2025.

sector within a third country[97]. In the absence of such adequacy decision, appropriate safeguards by the controller or the processor (the exporter of personal data) must be put in place[98]. Failing that, transnational personal data transfers are legal under the derogations provided for in the GDPR[99]. In any case, effective legal remedies for data subjects' rights must be available.

Appropriate safeguards can be binding corporate rules[100], standards data protection clauses adopted by the European Commission or by the national supervisory authority, codes of conduct, certifications mechanisms and *ad hoc* contractual clauses[101]. Binding corporate rules are general rules of a voluntary nature adopted by multinational groups, subsequently subject to approval by the national regulator of an EU Member State. Their application is global in nature within the business group, being mandatory for the entire group regardless of the countries where its branches or agencies were located. Standard contractual clauses are a model contract previously approved by the European Commission for the protection of personal data in transactions between companies located in third countries[102].

However, «supplementary measures» must be in place for the lack of protection in a non-EEA country[103]. Although the CJEU did not identify the measures, the EDPB guidance can be helpful for this complex task[104]. Only technical measures like encryption would impede access by foreign countries[105], but with limitations[106].

Article 49 GDPR also regulates the so-called «exceptions for specific situations» applicable in the absence of an adequacy decision or other appropriate safeguards. In the event of this circumstance, the international transfer of personal data will be lawful if there is explicit consent from the data subject[107]; the transfer is necessary for the performance of a contract[108]; there are important reasons of public interest[109]; the transfer is necessary for the exercise of a legal claim[110]; the purpose of the transfer is to protect vital interests of the data subject or of other

[97] The GDPR makes more flexible the data transfer regime in comparison with the Directive. *See* GDPR, Art. 45(1).
[98] GDPR, art. 46 (1).
[99] GDPR, art. 49.
[100] GDPR, art. 47.
[101] GDPR, art. 46 (2)-(3).
[102] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, *OJ*, L 199, 07.06.2021.
[103] *See* CORRALES COMPAGNUCCI, *et al*., «Supplementary Measures and Appropriate…», *op.cit.*, p. 153.
[104] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (20 November 2020), pp. 45-48.
[105] CORRALES COMPAGNUCCI, *et al*., «Supplementary Measures and Appropriate…», *op.cit*., p. 168.
[106] KORFF, Douwe, «Korff on Kuner: Schrems II Re-Examined», *Data protection and digital competition*, (3.09.2020), available at: https://www.ianbrown.tech/2020/09/03/korff-on-kuner-schrems-ii-re-examined/ For example, only in cases in which the data are not decrypted in the third country. Considering other tools such as organizational measures may not be very effective, as «few countries outside the EU meet the standards set by the Court when it comes to their national security agencies' powers of access to data (especially data on non-nationals) and lack of effective remedies».
[107] GDPR, art. 49(1)(a).
[108] GDPR, art. 49(1)(b) and (c).
[109] GDPR, art. 49(1)(d).
[110] GDPR, art. 49(1)(e).

persons who are physically or legally incapable of giving their consent[111], or the transfer is made from a public register with the purpose of providing information to the public or to a natural person who proves a legitimate interest, provided that, in each particular case, compliance with Union or Member State law regarding the consultation is guaranteed[112].

Nonetheless, these derogations are subject to strict conditions and usually for non-repetitive processing activities.[113] For example, the Dutch authority rejected Uber's attempt to rely on Article 49 GDPR derogations as the personal data transfers of drivers were neither «incidental» nor «necessary». The Dutch authority determined that the transfers between Uber U.S. and Uber Netherlands were systematic, repetitive, and ongoing[114]. Further, the Dutch authority found that the existence of a contract does not in itself constitute «necessity», and it suggested that Uber operated its data processing in the U.S. for efficiency reasons rather than necessity. Because Uber no longer used Standard Contractual Clauses from August 2021, the data of drivers from the EU were insufficiently protected, it had imposed a fine of 290 million euros ($324 million) on Uber On August 26, 2024[115]. This case exemplifies the problem of invalidating the Privacy Shield for U.S. companies that have violated the GDPR until they have self-certified under the new framework called the Data Privacy Framework.

Therefore, with respect to the State or territory that receives personal data, it is relevant to know if there is an adequacy decision by the European Commission. The United States has been included in such category by the European Commission's adequacy Decision of July 10, 2023, hereinafter, the Commission´s adequacy Decision or the Data Privacy Framework[116]. This would mean that it is not necessary to provide additional safeguards for international transfers from any EU country to the United States nor is an authorization from the national Data Protection Agency required.

However, in the absence of an adequacy decision, appropriate safeguards should be provided as prescribed by Article 46 of the GDPR, and national DPA are required to suspend or ban a data

[111] GDPR, art. 49(1)(f).
[112] GDPR, art. 49(1)(g).
[113] Jurcys, Paulius, Corrales Compagnucci, Marcelo, Fenwick, Marc, «The future of international data transfers: Managing legal risk with a 'user held' data model», *Computer Law & Security Review*, vol. 46, 2022, Article 105691, para. 2.1. https://doi.org/10.1016/j.clsr.2022.105691. But *see* Kuner, Christopher, «Schrems II Re-Examined», *Verfassungsblog* (25.08.2020), https://verfassungsblog.de/schrems-ii-re-examined/ («the derogations cannot fill the gap created by invalidation of the Privacy Shield, except in a few limited cases»), Rubinstein, Ira, Margulies, Peter, «Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground», *Connecticut Law Review*, vol. 54, 2022, pp. 518-456, p. 454 suggesting a combination of a risk-based approach and the derogation based on consent or performance of the contract for U.S. firms' EU employees.
[114] This transfer of data was the subject of a complaint by 172 French drivers to the French supervisory authority, the CNIL in 2020, which forwarded the complaint to the Dutch DPA, Uber's lead supervisory authority because Uber's European headquarters is in the Netherlands.
[115] Dutch Data Protection Authority, Press release, Dutch DPA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US, 26.08.2024, available at: https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us
[116] Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Brussels, 10.7.2023 C(2023) 4745 final https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

transfer data to a third country if, in their view, the SCC are not or cannot be complied with in that third country and the protection of data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer[117].

In the interim period between the invalidation of the Privacy Shield and the adoption of the Data Privacy Framework as an adequacy decision, the French Data Protection Authority (CNIL) prohibited the French national public health registry to be entrusted to servers run by Microsoft, or any of its subsidiaries, because U.S. companies were subject to U.S. national security laws. The French Conseil d'État required Microsoft to include a commitment for the company to follow the law of the EU, in granting access to public authorities to any data[118].

Moreover, the lack of an adequacy decision or the invalidity of the current adequacy decision could have costs for companies but also for institutions. The Regulation (EU) 2018/1725 created the European Data Protection Supervisor (EDPS) which is the independent supervisory authority for the protection of personal data and privacy and promoting good practice in the EU institutions and bodies. On 8 March 2024 the EDPS decision has found that the European Commission has infringed several key data protection rules when using Microsoft 365, including failing to provide appropriate safeguards to ensure that personal data transferred outside the EU[119] are afforded an essentially equivalent level of protection as guaranteed in the EU[120]. The EDPS decided to order the Commission, to suspend all data flows resulting from its use of Microsoft 365 to Microsoft and to its affiliates and sub-processors located in countries outside the EU, if not covered by an adequacy decision[121].

The recent *Bindl v Commission* case on 8 January 2025[122] illustrates the consequences of a claim for damages as a result of a personal data transfer to the United States. The General Court orders the Commission to pay damages to a visitor to its 'Conference on the Future of Europe' website because the displaying of the 'Sign in with Facebook' hyperlink on the EU Login website was entirely governed by the general terms and conditions of the Facebook platform. The key aspect is that at the time of that transfer, on 30 March 2022, there was no Commission Decision finding that the United States ensured an adequate level of protection for the personal data of EU citizens. Furthermore, the Commission has neither demonstrated nor claimed that there was an appropriate safeguard, in particular, a standard data protection clause or contractual clause[123].

[117] Schrems II, paras. 113-114.
[118] Corrales Compagnucci, *et al.*, «Supplementary Measures and Appropriate…», *op.cit.*, pp. 159-160.
[119] EU and EEA, European Economic Area, but for a simpler analysis, I only referred to EU.
[120] EDPS investigation into use of Microsoft 365 by the European Commission (Case 2021-0518), 8 March 2024, available at: https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf.
[121] The date of effectiveness was on 9 December 2024. The Commission sued the EDPS on 17 May 2024 – Commission v EDPS, T-262/24 (pending). But the EDPS follows up on the compliance of European Commission's use of Microsoft 365 on 10 December 2024, available at: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-follows-compliance-european-commissions-use-microsoft-365_en
[122] Judgment of the General Court in case T-354/22, *Bindl v Commission,* (8.01.2025), ECLI:EU:T:2025:4.
[123] Press release No. 25. Luxembourg 8 January 2025.

Given that it is the first time that the European Commission issued an adequacy decision following the General Data Protection Regulation (EU Regulation 2016/679 of April 27, 2016) with respect to transfers from the European Union to the United States, in the subsequent pages the adequacy Decision of July 10, 2023, on the EU-U.S. Data Privacy Framework is analyzed.

### 2.2. The EU-U.S. Data Privacy Framework

#### *a. The EU Commission press announcement*

Delving into the recent EU-U.S. Data Privacy Framework aims to avoid possible violations of individuals' privacy regarding their personal data. President Ursula von der Leyen said: «*The new EU-U.S. Data Privacy Framework will ensure safe data flows for Europeans and bring legal certainty to companies on both sides of the Atlantic. Following the agreement in principle I reached with President Biden last year, the US has implemented unprecedented commitments to establish the new framework. Today we take an important step to provide trust to citizens that their data is safe, to deepen our economic ties between the EU and the US, and at the same time to reaffirm our shared values. It shows that by working together, we can address the most complex issues*».[124]

According to the European Commission website: «The EU-U.S. Data Privacy Framework introduces new binding safeguards to address all the concerns raised by the European Court of Justice, including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC), to which EU individuals will have access. The new framework introduces significant improvements compared to the mechanism that existed under the Privacy Shield. For example, if the DPRC finds that data was collected in violation of the new safeguards, it will be able to order the deletion of the data. The new safeguards in the area of government access to data will complement the obligations that U.S. companies importing data from EU will have to subscribe to» [125].

#### *b. Preliminary criticism*

There are several errors in this press release dated July 10, 2023. The first is of a technical nature, since the data is not «EU data» as the statement states, but from the Europeans who are the subjects whose data is protected by European Union legislation. The rest of statements are counterargued throughout this study, so that the reader can understand to what extent the Commission is not faithful to European Union Law.

Firstly, it is necessary for companies operating on both sides of the Atlantic to adapt to requirements and safeguards established in this new mechanism. Therefore, are there new requirements? Companies can apply for certification on the EU-U.S. Data Privacy Framework website and must comply with data protection obligations. They must re-certify each year to continue benefiting from the new «Privacy Framework», being able to transfer data from the EU to the United States without additional safeguards. It has been acknowledged that tech giants

[124] European Commission, Press release, «Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows», 10.07.2023, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721
[125] *Ibid.*

lobbied for a replacement of the Privacy Shield, which explains part of the rush to adopt an adequacy decision[126]. However, another option would have been to continue negotiations with the United States to address the CJEU's concerns[127].

Second, the new privacy framework is also administered by the United States Department of Commerce like the old Privacy Shield. The U.S. Department of Commerce will process certification applications and monitor whether participating companies continue to meet self-certification requirements.

Thirdly, it is notable that the European Commission will continue to review the new Adequacy Decision periodically. During the first review in October 2024, the European Commission has verified whether all relevant elements of the U.S. legal framework are working effectively in practice[128]. Based on the results of such a review, the Commission has decided to carry out the next periodic review after three years, therefore, in July 2027[129]. This decision is welcome by the EDPB because a review in three years rather than the mandatory four years would allow EU institutions to obtain more speedly comprenhesive information about the practical application of the DPF [130].

In addition, the adequacy Decision can be adapted or even withdrawn, in the event of changes that affect the U.S. protective level. This entails a high risk for companies, considering that some of the safeguards of the adequacy Decision are encapsulated in an Executive Order under U.S. law, which may be modified, revoked or superseded by the President of the United States[131]. Besides, practical application and factual reality through the U.S. Supreme Court judgments play a predominant role here, and not only possible modifications at the legislative level. However, the Data Privacy Framework Decision is binding on the supervisory authorities in so far as it finds that the United States ensures an adequate level of protection and, therefore, has the effect of authorising personal data transferred under the DPF.

## 3. The Commission adequacy Decision 2023/1795

### 3.1. Formal issues

The Commission adequacy Decision 2023/1795 has 223 recitals, only four articles in less than two pages, six annexes, plus the principles and an annex of abbreviations. A total of 112 pages

[126] *See* VOSS, W. Gregory, «Transatlantic Data Transfer Compliance», *Boston University Journal of Sciences and Technology Law*, vol. 28, 2022, pp. 158-214, p. 177.
[127] *See* GERKE, Sara, REZAEIKHONAKDAR, Delaram, «Privacy Shield 2.0 — A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States», *Cardozo Law Review*, vol. 45, no. 2, 2023, pp. 351-403.
[128] *See infra* section 4.2 (a).
[129] EUROPEAN COMMISSION, Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework, Brussels, 9.10.2024, COM(2024) 451 final, p. 21.
[130] EUROPEAN DATA PROTECTION BOARD, Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, version 1.1., 4 november 2024, p. 23. *See infra* section 4.2 (b).
[131] *See* VOSS, «Transatlantic Data…», *op.cit.,* p. 178.

while the first Adequacy Decision had 41 pages[132] and the second Adequacy Decision had 112 pages[133]. This formal description introduces us to poor regulation of transatlantic data flows. The number of recitals is still innumerable, and even unnecessary. However, they give a good account of the European Commission intention and its position regarding data transfers to the United States. The European Commission interprets the jurisprudence of the Court of Justice of the European Union in a biased way and shields the recourse by national data protection authorities to not implement their Decision, for example, by blocking transfers to the USA and forcing them to resort to national courts. This is so, because the Decision is presumed legal and produces legal effects until it is annulled in an annulment action or declared invalid following a preliminary ruling or a ground of illegality before the courts of the Union[134].

U.S. organizations have to comply with seven basic Principles (notice, choice, accountability for onward transfers, security, data integrity and purpose limitation, data access and recourse, liability and effective enforcement regulation) and sixteen supplemental Principles. The Supplementary Principles address specific subjects, sensitive data, exceptions arising from freedom of the press, exemption from subsidiary liability of internet service providers, the exercise of due diligence and the conduct of audits for which the consent or knowledge of the data subject is not required, the role of data protection authorities, the principle of self-certification, verification through monitoring procedures, limitations on the right of access, human resources data, binding contracts for onward transfers, the establishment of a dispute resolution and enforcement mechanism, time limit for exercising the right to object, travel information, medical and pharmaceutical products, information from public records and publicly accessible information and access requests by public authorities. The certification mechanism for companies that adhere to the principle is set in an annex. There is a correlation of the principles listed in Chapter II of the GDPR[135].

Firstly, the Decision refers to the legal basis found in the General Data Protection Regulation[136] article 45(3), since this article grants the European Commission jurisdiction to issue an adequacy decision on a third country, therefore, outside the EU and to the European Economic Area, provided that such country is considered to guarantee an adequate level of protection. The GDPR refers to a country or one or more specified sectors within that third country, but the European Commission will set out, starting from recital 9 of the Decision, a self-certification system for U.S. organizations through the U.S. Department of Commerce.

---

[132] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), *OJ L 215, 25/08/2000*.

[133] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance), C/2016/4176, *OJ L 207, 1.8.2016*.

[134] Commission's Adequacy Decision, Recitals 205-206.

[135] BATLLE, Sergi, and VAN WAEYENBERGE, Arnaud, «EU–US Data Privacy Framework: A First Legal Assessment», *European Journal of Risk Regulation*, vol. 15, 2024, pp. 191–200, p. 194.

[136] EU Regulation 2016/679 of April 27, 2016.

First point of inconsistency, we are not facing a common Decision, but rather an *ad hoc* system that arises from the old Safe Harbor principles, which were invalidated when Decision 2000/520 was invalidated by the Court of Justice of the European Union in the Schrems I case[137]. Later in recital 6, reference is made to the fact that the framework has been updated, which is evident proof that Safe Harbor Principles continue but they are encapsulated in a new Adequacy Decision. Furthermore, these are organizations certified in the United States, and despite claiming to be based on the CJEU's jurisprudence, in particular, a system of self-certifications can guarantee an adequate level of protection (Schrems I), it is not being considered that the Privacy Shield was not equivalent to EU Law (Schrems II)[138]. Thus, the Commission's Decision gives rise to confusion; because it is a framework only for authorized entities in the U.S., when it would be logical for the European Commission to guarantee that the U.S. has an adequate level of protection and that it is equivalent to EU law.

Secondly, it refers to article 45(2) of the General Data Protection Regulation to remember that an adequacy Decision must be based on a substantive analysis of the legal system of the third State, including both rules applicable to data importers and guarantees with regarding access by public authorities to personal data. On the one hand, it is introduced that an «essentially equivalent» protection examination is going to be carried out in accordance with the GDPR and the jurisprudence of the CJEU[139], when in reality, the European Commission is based on its own Communication of January 10, 2017[140] that curiously, it also contradicts the Decision itself approved in 2023[141]; and it does not fully take into account either the European Parliament or the European Data Protection Board (EDPB), with the exception of partial references, such as, for example, the «Adequacy Referencial» of the EDPB[142]. It should be noted that the EDPB is an independent European body, being the coordinator of the national data protection authorities of the European Economic Area countries.

### 3.2. Searching for equivalent protection

#### *a. Data protection and privacy relationship*

The European Commission states that the United States has an equivalent level of protection to that of the European Union in Article 1 of the Adequacy Decision. However, an in-depth analysis does not seem to yield such a result. From a linguistic point of view, for example, «Data Privacy» translates as «privacidad de datos» in the Spanish version of the Adequacy Decision, which is

[137] *See supra* section 1.2.
[138] *See supra* section 1.3.
[139] Commission's adequacy Decision, Recital 3.
[140] EUROPEAN COMMISSION, Communication from the Commission to the European Parliament and the Council, *Exchanging and Protecting Personal Data in a Globalised World*, COM (2017)7, 10.1.2017.
[141] It states that the adequacy examination should not be point by point, but rather focus on the materiality of data protection rights and their effective implementation, supervision and enforcement, since the foreign system must provide a required level of protection, according to the Recital 4 of the Decision; but the framework with the U.S. is based on a system of self-certification of organizations, so non-certified US organizations do not fall into the framework.
[142] EUROPEAN DATA PROTECTION BOARD, Adequacy Referential, WP 254 rev. 01., available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

incorrect because under EU law there are two different rights: «data protection»[143] and «privacy»[144].

Article 7 of the EU Charter of Fundamental Rights provides that everyone has the right to respect for his or her private and family life, home, and communications. This is protected similarly under Article 8 of the European Convention of Human Rights[145]. Moreover, it can be protected as a general principle of EU law[146]. In addition, Article 8 of the EU Charter specifically addresses the fundamental right to the protection of personal data. There is no corresponding provision on data protection in the ECHR[147] but the European Court of Human Rights has covered data protection under Article 8 of the ECHR. Therefore, «private life» is not interpreted restrictively under the jurisprudence on the Court of Strasbourg and the Court of Luxembourg.

However, to what extent has U.S. law evolved regarding privacy or data protection? Precisely legal terminology is different. Does this mean substantial differences in the protection of fundamental rights? As it has been pointed, the external dimension of data flows is uneven. The EU regime proposes restrictions on data flows to third States to ensure that the level of protection of natural persons is not undermined[148]. Therefore, article 44 of the GDPR prohibits transfer of personal data to countries outside the borders of the EU, unless the receiving country can demonstrate a level of data protection equivalent to that of the EU. In contrast, U.S. law does not require a national regulator to approve a personal data transfer agreement[149]. This has practical implications, considering the market power of U.S. companies in online services. For example, technology giants such as Meta and Google allow access to personal information. Yet, the United States is one of the non-European G20 countries that does not have data protection laws that comply with Convention 108, which is the minimum international standard for most OECD countries[150].

[143] The whole linguistic problem derives from the translation of «privacy» as privacidad, but in Spanish only exists «*intimidad*» as a right. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) *Official Journal L 201, 31/07/2002.* Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. In French «*la protection de la vie privée*», in German «*Schutz der Privatsphäre*».

[144] PURTOVA, Nadezhda, *Property Rights in Personal Data, A European Perspective*, Alphen aan den Rijn, Wolter Kluwer, 2012, pp. 226-227: «Privacy labelled as an opacity tool is therefore a negative right which empowers an individual to prevent the State from intervening in his affairs, but not to require the State to take any positive steps. Data protection is a transparency tool. It does not prohibit State intervention, but rather channels and controls it by giving an individual positive rights and imposing affirmative obligations on the State».

[145] PURTOVA, *Property Rights…op.cit.*, pp. 227-240.

[146] KOKOTT, Juliane, SOBOTTA, Christoph, «The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR», *International Data Privacy Law*, 2013, Vol. 3, No. 4, pp. 222-228, p. 223.

[147] Only the Convention 108 of the Council of Europe specifically covers it but the ECtHR does not have jurisdiction on the Council of Europe Convention 108.

[148] *See supra* section 2.1.

[149] JIMÉNEZ-GÓMEZ, «Cross-Border Data…», *op.cit*., p. 4.

[150] GREENLEAF, Graham, «Global Data Privacy Laws 2023: 162 National Laws and 20 Bills», *UNSWLRS* 48, *Privacy Laws and Business International Report*, vol. 181, 2023, which specifies that the United States and India had notable failures to enact new laws in this period.

*b. U.S. law modifications*

*A. Safeguards for U.S. Signals Intelligence Activities*

14086 Executive Order entitled «Enhancing Safeguards for U.S. Signals Intelligence Activites» requires that signals intelligence activities have specific legitimate objectives. These objectives are in order to protect national security of the United States and of its allies and partners, understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability and geographic rivalry, protecting against foreign military capabilities and activities; against terrorism, the taking of hostages, and the holding of individuals captive by or on behalf of a foreign government, organisation or person; protecting against foreign espionage, sabotage, or assassination; protecting against threats from the development possession, or proliferation of weapons of mass destruction or related technologies and threats; protecting against cybersecurity threats created or exploited by, or malicious cyber activities, protecting against threats to the personnel of the U.S. or its allies or partners; protecting against transnational criminal threats, including illicit finance and sanctions evasion; protecting the integrity of elections and political processes, government property, and U.S. infrastructure and advancing collection or operational capabilities or activities in order to further a previous legitimate objective[151]. In addition, it explicitly prohibits such activities from being carried out for specific prohibited objectives (1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press; (2) suppressing or restricting legitimate privacy interests; (3) suppressing or restricting a right to legal counsel; or (4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion[152].

Moreover, it establishes novel procedures to ensure that signals intelligence activities contribute to the achievement of legitimate objectives and do not contribute to the achievement of prohibited objectives. For example, it requires that such activities be carried out only after determining, in a reasonable assessment of all relevant factors, that they are necessary to advance a validated intelligence priority and only in a manner proportionate to the validated intelligence priority for which they have been authorized[153]. Besides, it orders the services of the Intelligence Community to update their guidelines and procedures to incorporate the safeguards regarding signals intelligence established by the Executive Order. Finally, the Executive Order creates an independent and binding body that allows individuals in «Qualified States», designated pursuant to the Executive Order, to seek redress if they believe they have been subject to unlawful U.S. signals intelligence activities, including activities that violate the safeguards established in the Executive Order.

[151] Section 2(b)(i) EO 14086.

[152] Section 2(b)(ii) EO 14086.

[153] Adequacy Decision, Recital 135: «Before proposing intelligence priorities to the President, the Director National Intelligence must, in accordance with EO 14086, obtain an assessment from the ODNI CLPO for each priority as to whether it (1) advances one or more legitimate objectives listed in the EO; (2) was neither designed nor is anticipated to result in signals intelligence collection for a prohibited objective listed in the EO; and (3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside».

The Intelligence Community must apply the safeguards established in Executive Order No. 14086 to activities carried out under the article 702 of the Foreign Intelligence Surveillance Act (FISA). This Act allows the collection of foreign intelligence information regarding non-U.S. persons who are reasonably considered to be outside the U.S., with the obligatory assistance of electronic communication services companies. In principle, neither the Foreign Intelligence Surveillance Act (FISA) nor national security requirements allow mass data collection[154]. A judicial resolution is required to carry out electronic surveillance actions and physical records, except in restricted cases, such as emergency situations; and that it is always shown that there is probable cause to believe that the target is a foreign power or an agent of a foreign power[155]. In 2015, the Freedom Act modified Title IV of the FISA, which allowed devices to record outgoing and incoming communications if there was a judicial resolution, except in emergency situations, to require the Executive power to base its requests on specific selection criteria.

However, given that certain requirements are required to carry out «bulk collection» of personal information, the Intelligence Community can collect personal information on a bulk basis. «Bulk collection» means the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms)[156]. To this end, the Intelligence Community must apply reasonable methods and technical measures to limit the data that is collected to be necessary to advance the validated intelligence priority, which will minimize collection of irrelevant information[157]. Nevertheless, E.O. 14086 establishes a principle of equality between non-U.S. persons and U.S. persons regarding retention and delete of personal information[158]. Queries of bulk collection «take into account the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside»[159].

### *B. Data Protection Review Court composition*

The Data Protection Review Court is an «independent» quasi-judicial body established by the Secretary of Justice pursuant to Executive Order no. 14086. It is composed of at least six judges, appointed by the Secretary of Justice after consultation with the Privacy and Civil Liberties Oversight Board (PCLOB), the Secretary of Commerce and the Director of National Intelligence for renewable four-year terms[160]. Appointment of judges is based on criteria used by the executive branch when evaluating candidates for federal judiciary, with an assessment of previous judicial experience. In addition, judges must be legal professionals, that is, active members of the bar duly authorized to practice law and have appropriate experience in matters of privacy and national security regulations. However, not all magistrates must have been judges before, as only at least half of the magistrates are required to have experience, but it seems clear

[154] *See* Annex VII, Mr. Fonzone's letter December 9, 2022, Office of the Director of National Intelligence Office of General Counsel to the General Counsel of the US Department of Commerce.

[155] *See* 50 U.S. Code §§ 1805-1824.

[156] Executive Order 14086, section 4 (b).

[157] Executive Order 14086, section 2 (c) (iii) (D).

[158] Executive Order 14086, section 2 (c) (iii) (A)(2).

[159] Executive Order 14086, section 2 (c) (iii) (D).

[160] Attorney General Regulation on the Data Protection Review Court. 28 CFR Part 302.

that all judges must have the necessary security clearances to be able to access classified information of national security.

### *C. The Civil Liberties Protection Officer*

A new figure has been added within U.S. Intelligence: the Civil Liberties Protection Officer of the Director of National Intelligence (ODNI CLPO). The Privacy Framework does not mention that complaints must be qualifying according to EO 14086 sec 3.C(i). Assuming that complaints are qualified if they come from qualified States, the CLPO has jurisdiction for initiating investigation of individual complaints.

The ODNI CLPO is responsible for several functions, seeking to ensure that protection of civil liberties and privacy is appropriately integrated into the guidelines and procedures of the Office of the Director of National Intelligence and the intelligence services[161]. Some references are doubtful of the impartiality of the CLPO. When exercising its statutory and delegated authority to determine whether there was a covered violation, the Officer must take into account both relevant national security interests and applicable privacy protections; giving appropriate deference to any relevant determinations made by national security officials, applying the law impartially[162]. If the Executive Order specifically states that the Officer must apply the law impartially when it supposes to judge the situation of an individual whose personal information has been processed maybe in a bulk collection, is it not understandable that the law must apply impartially? Or is it not possible to apply the law impartially after giving deference to determination made by national security officials?

On the other hand, the CLPO must determine the appropriate remediation for any covered violation. But this determination is a classified report on information indicating a violation of any authority subject to the oversight of the Foreign Intelligence Surveillance Court (FISC) to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure[163].

In summary, the CLPO oversees compliance with applicable civil liberties and privacy obligations. He conducts privacy impact assessments. The same person must issue a report in which he must apply the regulations impartially, considering national security interests in signals intelligence activities and privacy protection. The ODNI CLPO's report must determine whether a violation of applicable U.S. regulations has occurred and, if so, will dictate appropriate remedial measures. The following types of measures are considered «appropriate»: measures that fully remedy the detected violation, such as putting an end to illicit collection of data, deleting data collected illegally, eliminating queries' results carried out inappropriately on data lawfully collected by other means, restrict access to lawfully collected data to properly trained personnel, or withdraw intelligence reports that contain data obtained without sufficient authorization or

[161] Commission's Adequacy Decision, Recital 179: «responsible for ensuring that the protection of civil liberties and privacy is appropriately incorporated in policies and procedures of the ODNI and intelligence agencies; overseeing compliance by the ODNI with applicable civil liberties and privacy requirements; and conducting privacy impact assessment».
[162] EO 14086 sec 3.C(i)(B).
[163] EO 14086 sec 3.C(i)(D)

that have been illicitly disseminated. It is stated that the decisions of the ODNI CLPO are binding on the specific intelligence services[164]. However, the decisions are classified material[165]. Subsequently, the complainant is informed of the possibility of appealing to the Data Protection Review Court to review the ODNI CLPO's determinations[166].

*D. The special advocate*

In the event of an appeal to the Court, a special advocate is selected to ensure that the complainant's interests are represented and that the DPRC panel is well informed about all relevant issues of law and fact[167]. The special advocate is not appointed by the claimant but by the Attorney General, in consultation with the Secretary of Commerce, the Director of National intelligence, and the Privacy and Civil Liberties Oversight Board[168], for two-renewable terms.[169] Although the Special Advocate has access to all information relating to the case, including classified information[170], he does not have an attorney-client relationship with the complainant.

*E. The Data Protection Review Court intervention*

Finally, the Data Protection Review Court reviews the decisions of ODNI CLPO, whether there has been a violation of the applicable U.S. regulations or whether the remedy has been adequate[171]. The Data Protection Review Court can issue its own determinations if they disagree with the determinations of the ODNI CLPO. Despite these virtues, according to the European Data Protection Board, it is a court that carries out secret decisions and violates the right of citizens to access and rectify data about them[172].

Furthermore, this court does not have full independence[173]. Some authors express that while that the new redress procedure is an improvement over the status quo, it is unlikely to meet EU law's «independence» standard, which requires a judicial body to operate «wholly autonomously» and free from «any hierarchical constraint.»[174] However, other authors state that «under the U.S. legal

[164] Section 3(c)(d) EO 14086.
[165] Section 3(c)(i)(F)-(G) EO 14086.
[166] Sections 3(c)(i)(E)(2)-(3) EO 14086.
[167] Section 3(d)(i)(C) EO 14086 and Section 201.8(e) AG Regulation. [28 CFR §201.8(e)].
[168] 42 U.S.C. § 2000ee (g). The PCLOB is an independent agency within the executive branch composed of a bipartisan, five-member Board appointed by the President for a fixed six-year term with Senate approval. «According to its founding statute, the PCLOB is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protect privacy and civil liberties. In its review it can access all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony», Commission's Adequacy Decision, Recital 110.
[169] Section 201.4 AG Regulation.
[170] Section 201.8(c) and 201.11 AG Regulation.
[171] Section 3(d)(i)(E) EO 14086 and Section 201.9(c)-(e) AG Regulation.
[172] *See* EUROPEAN DATA PROTECTION BOARD, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 28.02.2023.
[173] NOYB, *European Commission gives EU-US data transfers third round at CJEU*, 10 July 2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu («which is not a court, but a partly independent executive body»).
[174] GORSKI, Ashley «The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance», *Just Security* (4 November 2022), https://www.justsecurity.org/83927/the-biden-

system, an agency-issued regulation has the binding force of law, making it a suitable vehicle for defining the procedures for the review of redress requests and complaints»[175]. In contrast to the previous ombudsperson, «the president has limited his discretion by issuing the executive order, which orders the attorney general to adopt a regulation creating an independent redress body. Such legal limits on the powers of the president and the attorney general remain operative for so long as the executive order and DOJ regulation remain in effect»[176]. Yet, the EU Commission finding of adecuacy should be conditioned on the existence of those limits[177].

### *F. Result on redress mechanism for unlawful surveillance*

The Attorney General Regulation establishes a specific path to process and resolve claims from individuals relating to U.S. signals intelligence activities. Any individual in the EU is entitled to file a complaint with the competent body in relation to possible violations of the U.S. regulations that regulate signals intelligence activities whenever they negatively affect their interests in terms of privacy and civil liberties. The U.S. regulations in this regard are made up of: Executive Order no. 14086, Executive Order no. 12333 and Article 702 of the Foreign Intelligence Surveillance Act. Only individuals from countries or regional economic integration organizations designated by the U.S. Attorney General as «qualifying states» can use this route. In this regard, the EU and the three EFTA countries that make up the EEA were designated by the U.S. Attorney General as «qualifying states» under Executive Order no. 14086[178].

It should be noted that the procedure is not direct before the U.S. Data Protection Review Court. First, EU data subjects who want to make such a complaint must send it to the national data protection authority of the EU Member State responsible for supervising their personal data processing. Although this guarantees an easy way to challenge, since individuals can contact a nearby authority with which they can communicate in their own language[179], it should be noted that it lengthens the procedure since the national data protection authority only channels the claim to the corresponding body through the Secretariat of the European Data Protection Board. In principle, admissibility requirements of claims are not demanding, since individuals do not need to demonstrate that their data has actually been the subject of U.S. signals intelligence activities[180]. However, evidence must be shown regarding the belief that personal data has been

administrations-sigint-executive-order-part-ii/; BATLLE, Sergi, and VAN WAEYENBERGE, Arnaud «EU–US Data Privacy Framework: A First Legal Assessment», *European Journal of Risk Regulation*, vol. 15, 2024, pp. 191–200, p. 198. GERKE, Sara, REZAEIKHONAKDAR, Delaram, «Privacy Shield 2.0 ...», *op.cit.*, p. 398.

[175] CHRISTAKIS, Theodore, PROPP, Kenneth & SWIRE, Peter, «The Redress Mechanism in the Privacy Shield Successor: On the Independence and Effective Powers of the DPRC», *IAPP.ORG* (2022), https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc. («To protect against arbitrary or sudden change, modifying or repealing the regulation would require following the same public procedural steps as enacting it in the first place as the Supreme Court found in Motor Vehicles Manufacturers Association v. State Farm Mutual Automobile Insurance Co»).

[176] Ibid.

[177] BARCZENTEWICZ, Mikolaj, «Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States» (September 25, 2023). International Center for Law & Economics Issue Brief 2023-09-25, p. 15, available at SSRN: https://ssrn.com/abstract=4585431

[178] *See* Commission's Adequacy Decision, Recital 176.

[179] Commission's Adequacy Decision, Recital 177 refers to an authority 'close to home'.

[180] *See* Section 4(k)(i)-(iv) EO 14086.

transferred to the U.S., as well as whether it is known which U.S. public bodies are believed to be involved in the alleged breach; the evidence to substantiate the allegation that a violation of U.S. regulations has occurred, and the nature of the reparation measure requested. It is mentioned that it is not necessary to prove that the U.S. intelligence services collected the personal data[181], but such proof may be impossible. Schrems called it the trick on redress, because the Ombudsperson mechanism of the Privacy Shield has been renamed and split to a Civil Liberties Protection Officer (CLPO) and so-called Court[182]. It has been called a dual administrative body[183]. The complaint is reviewed by the CLPO. However, the CLPO's answer does not state the grounds of its decision. It neither confirms nor deny if the complainant has been subject to US intelligence activities[184]. The CLPO is limited to find no violation, or instead, to request the implementation of appropriate measures. It will inform that the decision may be appeal to the DPRC, and eventually, a special attorney will represent the complainant's interests, but it will not be appointed by him.

The Court of Justice of the European Union would examine these U.S. legal modifications under the lenses of Article 52(3) of the EU Charter, which is intended to ensure the necessary consistency between the rights contained in the EU Charter and the corresponding rights guaranteed in the ECHR. The CJEU found that «account must be taken of the corresponding rights of the ECHR for the purpose of interpretating the Charter, as a minimum threshold of protection».[185]

Regarding bulk collection, the European Court of Human Rights (ECtHR) requires an independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review[186]. In *Big Brother Watch and Others v. the United Kingdom*, the ECtHR set the criteria for a bulk interception regime to be ECHR compliant under the domestic legal framework, that must clearly defined: 1. the grounds on which bulk interception may be authorised; 2. the circumstances in which an individual's communications may be intercepted; 3. the procedure to be followed for granting authorisation; 4. the procedures to be followed for selecting, examining and using intercept material; 5. the precautions to be taken when communicating the material to other parties; 6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed; 7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; 8. the procedures for independent ex post

[181] Commission's Adequacy Decision, Recital 178.
[182] NOYB, *European Commission gives EU-US data transfers third round at CJEU*, 10 July 2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu
[183] Batlle & van Waeyenberge, «EU–US Data Privacy Framework …», *op.cit.*, p. 195
[184] NOYB affirms that the «judgment» of its «Court» is known before the case is brought and that and they will give the exact same response as the previous «Ombudsperson». NOYB, *European Commission gives EU-US data transfers third round at CJEU*, 10 July 2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu
[185] C-511/18, C-512/8 and C-520/18, *La Quadrature du Net and Others*, Judgment of the Court (Grand Chamber) of 6 October 2020, ECLI:EU:C:2020:791.
[186] ECtHR (Grand Chamber), *Big Brother Watch and Others v. The United Kingdom*, 25.05.2021, para. 350, hereinafter Big Brother Watch judgment.

facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance[187].

Therefore, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive, it does not need to be a court.[188] The European Court of Human Rights is not persuaded that «the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content»[189]. Thus, it considers that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content.

*c. Redress options for commercial matters*

Quantity of redress prevails over the quality of avenues of appeal in the EU-US Data Privacy Framework. Most mechanisms provide for a procedure in the U.S., which is not an advantage for a European citizen, although this has been alleviated with digitalization.

First, the individual must contact the U.S. organization that has been certified within the Privacy Framework. If the organization does not resolve the claim but it has designated an independent private entity for dispute resolution in its privacy policy, the claimant can follow this route.

Second, it is possible to direct the complaint to the U.S. authorities in charge of compliance. The individual must contact the Department of Commerce or the Federal Trade Commission. The Department of Commerce does not have the power to impose fines, but if it finds non-compliance, it can delete the organization from the list of entities adhering to the Privacy Framework. The Federal Trade Commission only pursues against acts of unfair competition[190]. The Department of Transport is another U.S. enforcement authority but only in its area of responsibility. The Privacy Principles refer vaguely to other enforcement authorities; however, no further public authorities currently appear to exist and neither laws nor other prohibited acts are defined.

Third, the complainant can address the national data protection agency of the competent EU Member State, which is mandatory in the case of data relating to human resources collected in an employment relationship[191], where recourse to arbitration is excluded. In this case, it will be the national data protection agency that will oversee making a complaint to the U.S. organization that adheres to the Privacy Framework. U.S. member organizations that have chosen this mechanism must pay a fee to cover coordination with European data protection authorities.

[187] Big Brother Watch judgment, para. 361.
[188] Big Brother Watch judgment, para. 351.
[189] Big Brother Watch judgment, para. 363.
[190] STUCKE, Maurice E., «Addresing Personal Data Collection as Unfair Methods of Competition», *Berkeley Technology Law Journal*, vol. 38, issue 2, 2023, pp. 717-795. The FTC cannot fix the surveillance economy with its authority under the FTC Act. United States still needs an overarching privacy framework. But the FTC can help close the regulatory gap by exercising the authority that Congress intended it to exercise to help curb data monopolies.
[191] *See* Commission Adequacy Decision, Recital 67.

Fourth, binding arbitration may be used as a last resort, but the arbitrators will be seated in the U.S. and the award can only be reviewed by U.S. courts[192]. These must be residual complaints that are unresolved or partially resolved. One of the main shortcomings is that individuals cannot use the mechanism for exceptions to the Privacy Framework Principles or to challenge the adequacy of the Privacy Framework[193].

### 3.3. **Zooming on selected data protection issues in the U.S.**

#### *a. State privacy law*

Privacy laws in the United States are sector-specific, protecting consumers by regulating certain financial data, health data, telecommunications data, and data collected by the government. Although these laws provide consumers with specific data protections, these protections are limited in scope and there is no central agency responsible for enforcing them. So far only seven states (California[194], Colorado[195], Connecticut[196], Utah[197], Virginia[198], Texas[199] and Montana[200]) have comprehensive privacy laws in place. Most of states acts do not afford a private right of action, except the California Consumer Privacy Act (CCPA) that gives individuals the right to seek statutory damages[201] against a business but only if the consumer is a California resident[202]. In a comparative sense, the general definition of «personal information» under the CCPA/CPRA is similar to the GDPR definition of «personal data». Yet, the definition of personal information

---

[192] *See* JIMÉNEZ-GÓMEZ, Briseida Sofía, «Arbitraje sobre controversias de protección de datos en el acuerdo entre los Estados Unidos y la UE», *La Ley: Mediación y Arbitraje*, núm. 21, 2024, pp. 1-45.

[193] *Ibid*.

[194] Cal. Civ. Code §1798.100 et seq. (Effective since 1 Jan. 2020). The California Consumers Privacy Act (CCPA) and later, the California Privacy Rights Act (CPRA, into effect on 1 Jan. 2023) creates the first data protection authority in the United States: the California Privacy Protection Agency (CPPA). From 1 July 2023 businesses can be fined for violations of the CPRA by the California Privacy Protection Agency.

[195] Colo. Rev. Stat. § 6-1-1301. (Effective since 1 July 2023).

[196] Conn. Gen. Stat. §§ 42-515—425-526. (Effective since 1 July 2023).

[197] Utah Code § 13-61-101 et seq. (Effective since 31 Dec. 2023).

[198] Va. Code §§ 59.1-571—59.1-581 (Effective since 1 Jan. 2023).

[199] Tex. Bus. & Com. Code §§ 541.001-541.005 (Effective since 1 July 2024).

[200] Mont. Code §§30-14-2801—30-14-2817 (Effective since 1 Oct. 2024).

[201] Cal. Civ. Code §1798.150 Statutory damages will be calculated as an amount between $100 and $750, per consumer, per incident. Consumer can recover statutory damages or actual damages (losses that resulted directly from the business's failure to properly secure user data), whichever is greater. Since many data breaches involve other types of personal information, and actual damages can be difficult to prove claims for actual damages are likely to be less common than those for statutory damages. Statutory damages could be recovered if a consumer's credit card details are breached, so the money that is stolen from them would be actual damages.

[202] Many cases ended by withdrawal of the claim or by a proposed settlement, *Cullen v. Zoom Video Communications, Inc*., Civil Docket No. 5:20-cv-02155-LHK (N.D. Cal.) (wherein the plaintiffs initially alleged that Zoom violated the CCPA by improperly sharing their personal information with Facebook, Inc., though this claim was ultimately dropped from the recently amended complaint); *G.R. v. TikTok Inc., et al*., Civil Docket No. 1:20-cv-05212 (N.D. Ill.) (alleging that TikTok disclosed and/or disseminated biometric identifiers or biometric information to third parties without the plaintiff's consent). The CCPA claims against Zoom and TikTok have now been resolved (either by withdrawal of the claim or by a proposed settlement), but plaintiffs will undoubtedly continue trying to test the limits of the private cause of action. TRIFON, Tara L., KRESS, Lindsey E., «The Murky Waters of the CCPA's Private Right of Action: Real and Perceived Ambiguities Complicating Litigation», *Privacy & Cybersecurity Newsletter*, Nov. 2024, available at: https://www.lockelord.com/newsandevents/publications/2020/11/the-murky-waters

subject to the safeguarding and private right of action provision for data breaches is narrower than the general definition of personal information[203]. Therefore, this is not a venue for Europeans.

Absence of complete state legislation in the fifty States means that companies are also unclear about what they must comply with and are concerned about the cost that this will entail. Indeed, there is also no uniformity in U.S. state legislation or in the agencies responsible for enforcing such laws, compounded by lack of legitimacy to act on the application of private rights of action.

*b. U.S. law progress in automated processing*

17 U.S. States have adopted laws on automated processing and generally allowing opt-outs for certain types of decision-making based on profiling[204]. While there are differences in what is meant by «profiling» between the different States, profiling is generally defined as any form of automated processing performed on personal data to evaluate, analyse, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. Delaware adds a person's «demographic characteristics», and Indiana includes characteristics of health records. Indiana, Tennessee, and Texas limit the definition to «solely automated processing.» However, the new comprehensive privacy laws of Iowa and Utah have no specific provisions on the use of AI for profiling or otherwise. The laws of Connecticut, Delaware, Indiana, Montana, Tennessee, Texas, and Virginia are largely the same. California, Colorado, Florida, and Oregon have some significant differences[205]. It is typically consumers that can opt-out for profiling.

[203] *See* Cal. Civ. Code Section 1798.81.5(d)(1)(A) An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information. (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (vii) Genetic data. (B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

[204] Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (Del. Code Ann. tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Maryland Online Data Privacy Act of 2024, enacted May 9, 2024), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Island Data Transparency and Privacy Protection Act, enacted June 29, 2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051), and Virginia (Va. Code Ann. § 59.1-577).

[205] DODSON, Christopher, «Artificial Intelligence Systems, Profiling, and the New U.S. State Privacy Laws», Cyberlawmonitor, 21.09.2023, available at: https://www.cyberlawmonitor.com/2023/09/21/artificial-intelligence-systems-profiling-and-the-new-u-s-state-privacy-laws/ accessed 6.01.2025.

The FTC has been active with the first enforcement action by the agency that addresses alleged discrimination through the use of automated decision-making technologies[206]. For example, Rite Aid used surveillance technologies for theft deterrence purposes that involved algorithmic unfairness. Rite Aid agreed to cease using facial recognition or analysis systems for five years and established a monitoring program to address risks if it seeks to use such systems for certain purposes in the future[207]. The AI was used in an allegedly discriminatory manner that were likely to cause substantial injury to consumers.

Moreover, the FTC has a more proactive enforcement approach on th protection on sensitive data. In 2024 two cases are relevant for health data. First, the FTC has prohibited data broker X-Mode and its successor Outlogic from sharing or selling any sensitive location data to settle allegations that the company sold precise location data that could be used to track people's visits to sensitive locations such as medical and reproductive health clinics and places of worship[208]. Second, the FTC against Monument that disclosed its users personal information (online alcohol addiction treatment service) to third party advertising platforms (like Meta and Google) via tracking technologies for advertising and third party marketing purposes[209].

*c. Lack of general federal law on data privacy*

The U.S. Congress failed to enact the American Data Privacy and Protection Act (ADPPA) in the waning days of the Democratic majority in the House of Representatives. The bill as written would have been the first comprehensive data protection law in the United States, except that it had several flaws from a global perspective: it only protected personal data of American citizens[210], and it left loopholes related to transfers between public and private sectors. Furthermore, the ADPPA federal regulation would have primacy and it would prevent any State from applying legal provisions that cover the same matters as the ADPPA, or even modifying state laws to make them better, that is, to continue advancing the protection of privacy rights. It is not surprising that scholars started to advise to enact a comprehensive federal privacy law[211]. It will help to create a harmonized approach to data protection in the United States, as the current situation is described as a labyrinth of privacy laws at the state level[212]. This federal privacy law would eliminate the costs of companies to comply with U.S. law and it will also provide adequate protection to all data subjects in the U.S., not just those residing in states with comprehensive privacy laws.

---

[206] Federal Trade Commission v. Rite Aid Corporation, Complaint for permanent injuction and other relief, 19.12.2023, https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf

[207] SHEN, Lei, *et al*., «FTC Targets Algorithmic Discrimination in Settlement With Rite Aid», *Cooley*, 24.01.2024, https://cdp.cooley.com/ftc-targets-algorithmic-discrimination-in-settlement-with-rite-aid/

[208] FEDERAL TRADE COMMISSION, Decision and Order, against X-Mode Social and Outlogic, Inc., and LLC, 11.04.2024, https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf

[209] Complaint for permanent injunction, civil penalty judgment, and other relief, 4.11.2024, https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentComplaintFiled.pdf

[210] GREENLEAF, Graham, «Proposed US federal data privacy law offers strong protections but only to US residents», *Privacy Laws & Business International Report,* vol. 179, no. 1, 2022, pp. 3-7. UNSW Law Research Paper No. 22-50, available at SSRN: https://ssrn.com/abstract=4342518

GREENLEAF, Graham, «Global Data Privacy Laws 2023: 162 National Laws and 20 Bills», *Privacy Laws and Business International Report*, vol. 181, no. 1, 2023, pp. 2-4, p. 3, UNSW Law Research Paper No. 23-48, available at SSRN: https://ssrn.com/abstract=4426146

[211] GERKE & REZAEIKHONAKDAR, «Privacy Shield 2.0 …», *op.cit*., p. 400.

[212] *Ibid*., p. 400.

*d. Standing before the U.S. Supreme Court*

It should be noted that addressing ordinary U.S. courts to claim illegalities in terms of data protection is not easy. One obstacle turns out to be proving standing of the individual in the U.S. Supreme Court jurisprudence. Any individual, regardless of their nationality, must prove three aspects[213]. First, suffering a *de facto* injury by the individual. Second, causal connection between the harm and the controversial conduct. Third, it is more likely than speculative that a favorable decision by the court will address the harm[214]. For the purposes of this study, it is significant to note that the U.S. Supreme Court has restricted the doctrine of standing, preventing issues about «privacy» from reaching cassation[215].

An example is the case of *Ramirez v. TransUnion*[216]. Ramirez filed suit against TransUnion in the United States District Court for the Northern District of California, alleging that the OFAC list violated the Fair Credit Reporting Act (FCRA). This law was established to allow victims of false credit reports to seek avenues for redress. The agency incorrectly placed terrorist alerts on the first page of consumers' credit reports and subsequently sent them confusing and incomplete information about the alerts and how to remove them. Ramírez managed to obtain class action status for his case, along with 8184 other people who were also compared to the OFAC (Office of Foreign Assets Control)[217] list because they shared a name and had been notified by TransUnion. On appeal they agree with Ramírez but the Supreme Court reviews the case and only those 1853 of the group members have the right to sue, that is, only those whose credit reports were shared with third parties and had demonstrated some type of damage, whether physical, monetary or immaterial, including damage to reputation[218].

It is questionable whether U.S. courts are the only jurisdiction where individuals can bring monetary actions for damages based on privacy issues and provided that the information has been obtained or disclosed unlawfully and deliberately. It should be noted that, according to the Commission's adequacy decision, European citizens cannot bring claims for damages in the European Union or before the competent courts of a Member State[219].

[213] Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992).

[214] ELLIOT, Summer, «There's No Understanding Standing for Privacy: An Analysis of *TransUnion v. Ramirez*», *Berkeley Technology Law Journal*, vol. 37, issue 4, 2023, pp. 1379-1411.

[215] *See* SOLOVE, Daniel J., KEATS CITRON, Danielle, «Standing and Privacy Harms: a critique of Transunion v. Ramirez», *Boston University Law Review Online*, vol. 101, 2021, pp. 62-71.

[216] *Ramirez v. TransUnion LLC*, No. 17-17244 (9th Cir. 2020). *Transunion LLC v. Ramirez*, 951 F. 3d 1008, reversed and remanded. Certiorari to the United States Court of Appeals for the Ninth Circuit No. 20–297. Hearing, March 30, 2021—Decided June 25, 2021.

[217] It is a financial watchdog under the U.S. Department of the Treasury. It deals with the implementation of U.S. international financial sanctions, especially in the context of protecting national security and in support of U.S. foreign policy.

[218] *Transunion LLC v. Ramirez*, 951 F. 3d 1008, reversed and remanded. Certiorari to the United States Court of Appeals for the Ninth Circuit No. 20–297.

[219] This has already been criticized by the EUROPEAN DATA PROTECTION BOARD, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 13.04.2016, 16/EN WP 238, p. 27.

e. Government's assertions of secrecy

The text of FISA lacks any reference to the state secrets privilege, suggesting that its passage did not alter the privilege. Regardless of whether the privilege arises from common law or the Constitution, Congress could not have abrogated it without clear statutory language[220]. In the case of surveillance, the U.S. government relies on state secrets privilege to make it exceedingly difficult to establish standing to challenge that surveillance in an ordinary U.S. federal court under Article III of the U.S. Constitution. As Gorski states: «In theory, an ordinary U.S. federal court under Article III of the U.S. Constitution would satisfy the standard of an "independent" and "impartial" tribunal to protect privacy rights. But once again, theory is belied by reality, because vanishingly few plaintiffs in U.S. surveillance cases ever have the merits of their claims heard by a judge or jury.»[221] It is a fact that «no civil lawsuit challenging the lawfulness of surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) or Executive Order 12333 has resulted in a U.S. court opinion addressing the legality of that surveillance. Nor has any litigant obtained a remedy of any kind for Section 702 or EO 12333 surveillance»[222], irrespective of the litigant's nationality.

## 4. The European institutions voice

### 4.1. Before passing the adequacy Decision

*a. The European Parliament opinion*

The European Parliament has been very active on the issue, highlighting its European Parliament Resolution, of May 20, 2021, on the Schrems II ruling[223]. The most notable position regarding the issue at hand is that the European Parliament took a position against it on May 11, 2023, specifically: «Concludes that the EU-US Data Privacy Framework fails to create essential equivalence in the level of protection; 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; calls on the Commission not to adopt the adequacy finding until all the recommendations made in this resolution and the EDPB opinion are fully implemented»[224].

It was clear that the United States is the only country that has no federal privacy law. However, the European Commission did not use the European Parliament concerns to pressure the United

[220] *Federal Bureau of Investigation v. Fazaga et al*, 595 US _ (2022), Mar 4, 2022.
[221] GORSKI, «The Biden Administration's SIGINT Executive Order…», *op.cit.*
[222] *Ibid*.
[223] EUROPEAN PARLIAMENT Resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html
[224] EUROPEAN PARLIAMENT Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), para. 19, available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html

States to make changes on the law. The Commission adequacy Decision in recital 222 is aware of this negative position, which, although it may not be binding, is still the position of the representatives of European citizens[225].

*b. The European Data Protection Board opinion*

Opinion 5/2023 on the draft Implementing Decision of the European Commission on the adequacy of the protection of personal data in accordance with the EU-US data privacy framework was adopted on February 28, 2023, by the European Data Protection Board (EDPB) [226]. The fundamental component of the Data Privacy Framework is the Supplemental principles (collectively referred to as «the Principles»).

The principles are also largely the same as those contained in the Privacy Shield project on which WG29 based its opinion in 2016. There are positive aspects of this new privacy framework, such as, for example, the clarification that the encrypted data is personal data.

However, some aspects of the EDPB Opinion are worth mentioning in line with the ideas supported in this work.

Firstly, the EDPB recalls that, to consider that there is an adequate level of protection, both Article 45 of the GDPR and the jurisprudence of the CJEU require that the legislation of the third country offers data subjects an essentially equivalent level of protection to the one guaranteed in the EU[227].

Secondly, the EDPB recommends that the Commission include in the draft Decision a clarification on the scope of application of exemptions, including the safeguards applicable under U.S. law. The EDPB points out that the structure of the annexes and their numbering makes it difficult to locate the information and consult it. This contributes to a complex general presentation of the new framework, which compiles, in its annexes, documents of different legal value and may hinder the correct understanding of the principles by the interested parties, the entities adhering to the principles and the protection authorities of data in the EU.

Thirdly, the EDPB emphasizes that terminology should be used consistently throughout the principles. Likewise, the definition of some essential terms is missing, such as «agent» which seems to be assimilated to «processor» in the GDPR, but this does not have to be the case[228].

Fourthly, there are also no guarantees for onward transfers[229], nor are there specific U.S. rules on automated decisions, in particular, the right of the individual to know the underlying logic to challenge the decision, and to obtain human intervention when the decision significantly affects him or her.

[225] With 306 votes in favor, 231 abstaining, and 27 against.

[226] European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 28.02.2023.

[227] *Ibid*, p. 2.

[228] *Ibid*, p. 3.

[229] *Ibid*., p. 3.

Finally, it is also notable that the level of protection of individuals seems to vary according to specific sectoral regulations, when these exist[230].

### 4.2. First review assessment of the adequacy Decision

*a. The European Commission report*

More than 2800 companies have been certified under the DPF by the DoC, only 33 applications have been rejected. The DoC has not detected issues of compliance during the first year of the DPF Principles. There have been very few number of complaints which suggests that individuals may not be aware of their rights or the mechanism to exercise them[231].

The Commission considers that U.S. authorities have put in place the structures and procedures to ensure that the DPF works. In the report the Commission expresses its intention to monitor amendments of Section 702 FISA and the nomination and appointment of members to the PCLOB to fill vacancies. Moreover, the Commission invites the DoC to monitor the supervision and compliance with the Principles, as well as the FTC to engage in a more active activity to the investigation of compliance by the certified companies. It also announces that both U.S. and EU authorities should cooperate to develop guidance on HR data and onward transfers.

*b. The European Data Protection Board opinion*

There are several points of concerns with the current DPF for the European Data Protection Board.

First, the lack of *ex officio* oversight and enforcement actions from U.S. authorities is mentioned, in particular, considering the very few complaints by concerned individuals that might trigger enforcement action[232]. Proactive enforcement actions by the DoC, the U.S. FTC and U.S. DoT is needed to ensure compliance with the principles because automated compliance tools cannot substitute investigations[233]. It is neither clear if inactive organisations (2600 listed) or organisations that withdrew the DPF had returned, deleted or retained personal data[234].

Second, regarding the independent recourse mechanisms, they have received only eight eligible complaints out of 113. The IRM reports do not specify how conflict of interests are precluded and they are not presented in standarised form[235]. None of the EU data protection authorities have received complaints from EU individuals concerning non-compliance with the DPF. Neither the

[230] *See supra* in this paper, section 3.3.
[231] EUROPEAN COMMISSION, *Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework*, Brussels, 9.10.2024, COM(2024) 451 final, p.7.
[232] EUROPEAN DATA PROTECTION BOARD, Report on the first review…, *op.cit*., p. 7.
[233] *Ibid.*, p. 7.
[234] *Ibid.*, p. 8.
[235] *Ibid.*, p. 8.

US DoC has received any complaint or referral from other authority. No binding arbitration has been started during the first review[236].

Third, concerning the accountability for onward transfers principle, it is stated that companies may not be aware of the requirements for transfers received from EU importers to third countries that do not benefit from an adequacy decision by the EU Commission[237]. These companies may be using tools to conduct onward transfers that «do not provide the same level of protection for the onward transferred personal data as the one guaranteed by the DPF Principles»[238].

Fourth, the interpretation of the concept of HR Data under the DPF is problematic. The EDPB defines HR data as «any personal data concerning an employee in the context of an employment relationship, irrespective of whether the data is transferred within a corporate group or to a different commercial operator». However, the DoC considers that only the processing of employees' data within a corporate group is HR Data under the DPF. The Principle refers to «personal information to its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the EU-U.S. DPF»[239]. Therefore, the DPF is not restricted to employees' data transfers of the same corporate group. This interpretation is relevant as EU data protection authorities have power to handle complaints on HR data in the jurisdiction where the employees work[240]. In addition, the U.S. organization (covered by the DPF) «must respond directly to such authorities with regard to the investigation and resolution of complaints»[241]. The DoC will develop guidance to U.S. companies to clarify these notions.

Fifth, on access and use of personal data transferred under the decision by U.S. public authorities, the EDPB needs to monitors the effects of the implementation of necessity and proportionality by the EO 14086[242]. The EDPB acknowledges that it is not in a position to fully assess that implementation[243] and it needs more information, including practical examples and changes in day-to-day operations of the agencies. The EDPB does not criticize the possibility to establish secret objectives for which signals intelligence collection activities can take place. However, it emphasized the need to implement independent oversight mechanisms. Apparently, the PCLOB may review secret updates of the list of legitimate objectives following a request for classified information[244]. Yet the EDPB emphasizes that collection data in bulk under U.S. law neither provides for a requirement of prior authorization by an independent authority nor for a systematic independent review by a court or an equivalent independent body[245]. Indeed, new

[236] For a thorough analysis of this arbitration, *see* JIMÉNEZ-GÓMEZ, «Arbitraje sobre controversias ...», *op.cit.*, pp. 1-45.
[237] EUROPEAN DATA PROTECTION BOARD, Report on the first review..., *op.cit*., p. 9.
[238] *Ibid*., p. 10.
[239] Section III, 9, (a), (i) of the Annex I of the DPF.
[240] Section III, 9, (d), (i) of the Annex I of the DPF.
[241] Principle 7 (b) Annex I of the DPF.
[242] EUROPEAN DATA PROTECTION BOARD, Report on the first review..., *op.cit*., p. 12.
[243] *Ibid*., p. 13.
[244] *Ibid*., p. 14.
[245] EUROPEAN DATA PROTECTION BOARD, Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, version 1.1., 4 november 2024, pp. 14-15.

European Court of Human Rights caselaw held on independent prior authorisation of secret surveillance measures[246]. The ECtHR considered that the existing authorisation procedure should be supplemented by other *post factum* procedural review mechanisms; for example, where the surveillance had not led to criminal proceedings, a remedy available to persons who were concerned that they had been subjected to surveillance, with the possibility of seeking judicial review and a separate review by an independent body. For example, in *Pietrzak and Bychawska-Siniarska and Others v. Poland,* Polish law did not appear to contain appropriate provisions in that regard; nor did it provide for an obligation to inform the person targeted by a surveillance measure, even after a certain period of time had elapsed, and even where this would not compromise the aim of the measure[247].

Sixth, RISAA (Reform Intelligence and Securing America Act) extends Section 702 FISA for two years (2023-2026). However, it did not incorporate the PCLOB's recommedation to codify additional safeguards[248]. Some problems are the inconsistency of the definition of «foreign intelligence» since it is different in the EO and Section 702 FISA, and the expansion of the definition of «electronic communication service provider», so new entities are required to disclosed personal information under Section 702 FISA. The new «electronic communication service provider» definition covers «any other service provider who has access to equipment that is being used or may be used to transmit or store wire or electronic communications». Apparently, this inclusion is to cover a type of service provider in the litigation before FISA courts, but the EDPB states that this definition is not sufficiently clear to know which companies are within the scope, and in any case, the risk depends on the volume of personal data handled by the companies under scope, not on the number of companies[249]. Moreover, the EDPB observes that RISA changes the role of amicus curiae before the FISC (U.S. Intelligence Service Court) and the FISCR (U.S. Intelligence Service Court of Review) as amici curiae are limited to addressing the specific issues identified by the court, but they should advice on the privacy interest as the data subject is not a party to the proceedings before the court[250].

Seventh, on effective redress mechanisms including the independence of the DPRC, the EDPB notes that it has not yet been triggered and the annual review of the Privacy and Civil Liberties Oversight Board (PCLOB) is still pending[251]. A general standard response by the DPRC to the complainant and the DPRC's decisions cannot be appealed are also issues of concern[252]. Moreover, President Trump recently fired the three democrats on the PCLOB[253]. Since these

[246] ECtHR (Section First), Pietrzak and Bychawska-Siniarska and Others v. Poland, 28.05.2025.
[247] *Ibid.*
[248] European Data Protection Board, Report on the first review..., *op.cit*., p. 15.
[249] *Ibid*., p. 17.
[250] *Ibid*., p. 18.
[251] *Ibid*., p. 19.
[252] *Ibid*., p. 19.
[253] This was after the EDPB opinion, *see* Nojeim, Greg, Lorenzo Perez, Silvia, «Trump's Sacking of PCLOB Members Threatens Data Privacy», *Lawfare*, 31 January 2025, available at https://www.lawfaremedia.org/article/trump-s-sacking-of-pclob-members-threatens-data-privacy;
NOYB, «US Cloud soon illegal? Trump punches first hole in EU-US Data Deal», 23 January 2025, available at: https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal

firings bring the Board to a sub-quorum level, they have the potential to significantly disrupt transatlantic transfers of personal data from the EU to the U.S. under the DPF.

Eighth, EO 14086 safeguards do not apply to the purchase of personal data by U.S. intelligence agencies. Other rules such as a binding Intelligency Policy Framework set standards for how intelligence agencies acquire and use commercially available information (CAI)[254]. This framework was released on 8 May 2024[255]. This recent framework does not provide for the principles of necessity and proportionality, nor does it address legal remedies. In addition, there is uncertainty about the extent of safeguards for non-U.S. persons[256].

## 5. Conclusion

The Commission adequacy Decision of 10 July 2023 finds that the United States provides an adequate level of protection for personal data transferred from the European Union to the United States. This legal instruments binds on all the Member States of the EU and binds on all their organs, including national supervisory authorities. It produces the effect of authorizing such transfers of personal data, without additional requirements, that other alternative means such as SCC, BCR or codes of conducts need. US organizations have to comply with seven basic principles (notice, choice, accountability for onward transfers, security, data integrity and purpose limitation, data access and recourse, liability and effective enforcement regulation) and sixteen supplemental principles. The Supplementary Principles address specific subjects, sensitive data, exceptions arising from freedom of the press, exemption from subsidiary liability of internet service providers, the exercise of due diligence and the conduct of audits for which the consent or knowledge of the data subject is not required, the role of data protection authorities, the principle of self-certification, verification through monitoring procedures, limitations on the right of access, human resources data, binding contracts for onward transfers, the establishment of a dispute resolution and enforcement mechanism, time limit for exercising the right to object, travel information, medical and pharmaceutical products, information from public records and publicly accessible information and access requests by public authorities.

However, the Privacy Framework Principles are established to develop international trade, the only real interest of the U.S. The Privacy Framework Principles are parallel to U.S. or European law, so they do not affect either U.S. law or the EU Regulations of Data Protection. Furthermore, the Principles are voluntary for organizations that wish to join but once they self-certify, they

[254] CAI refers to the vast quantities of data—collected from a wide range of sources, including cell phones and other personal devices, cars, household appliances, and social media accounts—that are available for purchase from data brokers and other commercial entities. AYOUB, Emily, «Assessing the Intelligence Community's Policy Framework for Commercially Available Information», *Just Security*, May 24, 2024, https://www.justsecurity.org/96015/commercially-available-information/

[255] Some of the principles of the policy framework have been described as «simply restate basic constitutional requirements and constraints, calling into question the added value of including them in the policy. Moreover, …, the subjectivity and discretion built into many of these principles could allow IC agencies to prioritize "flexibility to experiment" with CAI over protecting Americans' privacy and civil liberties». AYOUB, «Assessing…», *op.cit*.

[256] *See* EUROPEAN DATA PROTECTION BOARD, Report on the first review…, *op.cit*., p. 21.

must comply with them. In essence, there has been little change from the original Safe Harbor Principles and the infamous Privacy Shield. Thus, the Privacy Framework is not available to insurance companies, financial institutions or nonprofit organizations, since they are not under the control of either the Federal Trade Commission or the U.S. Department of Transportation. Companies outside the Data Privacy Framework list do not benefit from the adequacy decision of the European Commision, which means they need to use alternative safeguards to transfer personal data like standard contractual clauses and binding corporate rules.

On the one hand, the shortcomings observed are that 14086 E.O. allows in some cases bulk collection of data (including communications content) using signals intelligence and does not provide for separate prior authorization for bulk collection. The assessment of whether the laws in question provide effective safeguards must be based not only on the laws as they exist in the corpus of legislation, but also on (a) the actual functioning of the surveillance regime and (b) the existence or absence of evidence of actual abuses[257]. The first periodic review of the Commission has showed that although the constitutive elements of the framework are in place, experience with the practical application of the safeguards is limited[258]. The EDPB maintains its concern on the lack of prior authorisation by an independent authority and the lack of a systematic independent *ex post* review by a court or equivalently independent body[259].

In addition, through trade and brokers, the U.S. government can access data with fewer protections than access through intelligence signals. Ongoing monitoring by the Privacy and Civil Liberties Oversight Board and the European Data Protection Board would reveal if the EO 14086 is not undermined. With Trump's return to the White House, members of the Privacy and Civil Liberties Oversight Board have already been removed.

At state level the United States has developed legislation on the automated processing of personal data and allows opt-outs for certain types of decision-making bases on profiling. In addition, several states have comprehensive privacy acts. However, there is not a federal privacy act in the United States, preventing a harmonized approach to data protection and causing hurdles to companies to comply with U.S. law. Moreover, standing and secrecy assertions by the government limits any decision by U.S. courts on privacy matters.

The Data Privacy Framework seems a temporal solution, as U.S. law is still developing in terms of access by public authorities to personal data transferred from the European Union to the United States. Congress passed the Reforming Intelligence and Securing America Act (RISAA) on 19 April 2024, re-authorising Section 702 FISA for 2 years. Section 702 FISA was set to expire at the end of 2023, but it continues targeting non-U.S. persons reasonably believed to be located outside the U.S. to acquire foreign intelligence information. The EDPB regrets that RISAA did not incorporate the PCLOB's recommendation to codify certain safeguards of EO 14086 in Section 702 FISA. First, the definition of foreign intelligence information has been expanded to include information related to counternarcotics. The definition of foreign intelligence should be

[257] ECtHR (Section First), Pietrzak and Bychawska-Siniarska and Others v. Poland, 28.05.2025., para.194.
[258] European Commission, Report on the first periodic review ...*op.cit*., p. 21.
[259] European Data Protection Board, Report on the first review ...*op.cit*., pp. 14-15.

aligned in the EO and Section 702 FISA and confer explicit jurisdiction to the FISC to enforce the EO when evaluating Section 702 FISA collection practices.

As the European Court of Human Rights has held «an effective remedy should be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime»[260]. Regarding concerns about redress mechanisms in the case of signals intelligence access, two layers of review are included in the President Biden's Executive Order on Enhancing Safeguards for Signals Intelligence Activities of October 7, 2022. Initially, the Civil Liberties Protection Officer who begins an investigation if a complaint is received, determining whether U.S. law, including Executive Order No. 14086, has been violated, whose novelty is the right of access for individuals. In a second stage, the Data Protection Review Court may intervene in matters of data protection, which establishes a final and binding decision. However, it must be considered that the complainant does not come into direct contact with the «Court of Appeal» on data protection matters.

In principle, the new DPRC will independently review determinations made by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence in response to «qualified» complaints submitted by citizens through «appropriate» public authorities, which they allege violations of U.S. law in the conduct of U.S. signals intelligence activities. However, as it has been analyzed, these mechanisms do not seem to be very transparent and the standard answer by the DPRC and the CLPO under EO 148086 remains a concern.

On the other hand, it is still very unfortunate that the U.S. President can modify the Executive Order on which the data protection guarantees towards the U.S. are based. Nor can its interpretation be predictable or clear since U.S. law enforcement, if such law exists, is left to chance since the U.S. does not have federal legislation on privacy, and how the new mechanisms are working in practice will be specified, having to wait for the next review report from the European Commission itself. In addition to these ambiguities, clear concerns about the independence of the Data Protection Review Court arises, where the President of the United States can also revoke decisions, which are secret, and these can also be revoked in secret. There is no transparency nor impartiality, no matter how much political agreements or letters from authorities try to remedy it with explanations, also included in the adequacy decision recitals on these judges' independence, when they are part of the executive branch and not the judicial branch. Therefore, with such interference between branches, there cannot be guarantee for independence of powers.

At a technical level, it is incoherent that the Court is called «data protection review court» and yet the necessary expertise is in «privacy», which, on the other hand, is the American term in its legislation. However, the Commission Decision only refers to «data protection» to refer to E.U. law.

Furthermore, although it is frequently said that the conditions of access by U.S. intelligence units will be in accordance with «necessity» and «proportionality» requirements, it seems that the

[260] Big Brother Watch and Others v. The United Kingdom, para. 357.

reference point is the U.S. legal system[261], while the Court of Justice has assessed «necessity» and «proportionality» of these measures in accordance with European Union law and, crucially, the EU Charter of Fundamental Rights. It is clear that a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards[262]. In this regard, on their interpretation and compliance relative to the DPF Principles, those doubtful issues are resolved in accordance with U.S. law, except when the participating organizations have shown their commitment to cooperate with the European data protection authorities. This exception introduces the possibility of not cooperating with the European data protection authorities and, nevertheless, being adhered to the Data Privacy Framework. This is possible because the dispute resolution mechanism is left to the organization's choice and it may be a panel established by the European data protection authorities, a private alternative resolution mechanism established in the EU or the United States. Thus, a U.S.-based dispute resolution service provider can be chosen, which could not be disputed by European citizens.

Finally, the Data Privacy Framework seems an improvement in comparison to the past situation (the Ombudsman mechanism, the more targeted objectives by Signal activities), but not robust enough to pass the examination of the Court of Justice of the European Union. An eventual invalidation of the new adequacy decision would require resorting to other transfer mechanisms, such as standard contractual clauses or binding corporate rules to be safe in personal data transfers to the United States, where competent courts could be directly included, which would facilitate avenues of appeal regarding data protection. The main disadvantage is that transatlantic data flows remain an unestable area with potential future impact in companies operating cross-border.

[261] 14086 Executive Order declares that FISA mass surveillance 702 is «proportionate» according to an undisclosed «U.S. interpretation» of the word and contrary to the two conclusions of the CJEU. In this way, the EU and the U.S. could affirm that they agreed on the same word («proportional»), even when there is no agreement on the meaning of the word.
[262] Schrems II, para. 180.

## 6. Bibliography

AKKERMANS, Bram, «The Influence of the Four (or Five) Freedoms on Property Law», in VAN ERP, Sjef and ZIMMERMANN, Katja (eds.), *Research Handbook on European Union Property Law,* Northampton, Edward Elgar Publishers, 2023 , accessed to the SSRN version, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4232332

AYOUB, Emily, «Assessing the Intelligence Community's Policy Framework for Commercially Available Information», *Just Security*, May 24, 2024**,** https://www.justsecurity.org/96015/commercially-available-information/

BARCZENTEWICZ, Mikolaj, «Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States» (September 25, 2023). International Center for Law & Economics Issue Brief 2023-09-25, available at SSRN: https://ssrn.com/abstract=4585431

BATLLE, Sergi, and VAN WAEYENBERGE, Arnaud «EU–US Data Privacy Framework: A First Legal Assessment, *European Journal of Risk Regulation*, vol. 15, 2024, pp. 191–200.

BRADFORD, Anu, *The Brussels Effect: How the European Union Rules de World*, Oxford University Press, 2020.

CHANDER, Anupam, SCHWARTZ, Paul M., «Privacy and/or Trade», *University Chicago Law Review*, vol. 90, issue 1, 2023, pp. 49-135.

CHRISTAKIS, Theodore, PROPP, Kenneth & SWIRE, Peter, «The Redress Mechanism in the Privacy Shield Successor: On the Independence and Effective Powers of the DPRC», *IAPP.ORG* (2022), https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc.

CORRALES COMPAGNUCCI, Marcelo, FENWICK, Marc, ABOY, Mateo AND MINSSEN, Timo, «Supplementary Measures and Appropriate Safegurds for International Transfers of Health Data After *Schrems* II», in M. Corrales Compagnucci et al. (eds), *The Law and Ethics of Data Sharing in Health Sciences, Perspectives in Law, Business and Innovation*, Springer, Singapor, 2024, pp. 151-171.

DODSON, Christopher, «Artificial Intelligence Systems, Profiling, and the New U.S. State Privacy Laws», *Cyberlawmonitor*, 21.09.2023, available at: https://www.cyberlawmonitor.com/2023/09/21/artificial-intelligence-systems-profiling-and-the-new-u-s-state-privacy-laws/

DUTCH DATA PROTECTION AUTHORITY, Press release, Dutch DPA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US, 26.08.2024, https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us

ELLIOT, Summer, «There's No Understanding Standing for Privacy: An Analysis of *TransUnion v. Ramirez*», *Berkeley Technology Law Journal*, vol. 37, issue 4, 2023, pp. 1379-1411.

EUROPEAN COMMISSION, Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework, Brussels, 9.10.2024, COM(2024) 451 final.

EUROPEAN COMMISSION, Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, COM/2024/7 final, Brussels, 15.1.2024.

EUROPEAN COMMISSION, Press release, «Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows», 10.07.2023, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

EUROPEAN COMMISSION, Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Brussels, 10.7.2023 C(2023) 4745 final https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

EUROPEAN COMMISSION, Communication from the Commission to the European Parliament and the Council, *Exchanging and Protecting Personal Data in a Globalised World*, COM (2017)7, 10.1.2017.

EUROPEAN DATA PROTECTION BOARD, Adequacy Referential, WP 254 rev. 01., available at https://ec.europa.eu/newsroom/article29/items/614108

EUROPEAN DATA PROTECTION BOARD, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 28.02.2023.

EUROPEAN DATA PROTECTION BOARD, Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, version 1.1., 4 november 2024.

EUROPEAN DATA PROTECTION SUPERVISOR, Press release, EDPS follows up on the compliance of European Commission's use of Microsoft 365 on 10 December 2024, 10.12.2023, https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-follows-compliance-european-commissions-use-microsoft-365_en

EUROPEAN DATA PROTECTION SUPERVISOR, EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II"), 17.07.2020, https://www.edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling_en

EUROPEAN PARLIAMENT, Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html

EUROPEAN PARLIAMENT, Resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html

FEDERAL TRADE COMMISSION V. RITE AID CORPORATION, COMPLAINT FOR PERMANENT INJUCTION AND OTHER RELIEF, 19.12.2023, https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf

FEDERAL TRADE COMMISSION, DECISION AND ORDER, AGAINST X-MODE SOCIAL AND OUTLOGIC, INC., AND LLC, 11.04.2024, https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf

GERKE, Sara, REZAEIKHONAKDAR, Delaram, «Privacy Shield 2.0 — A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States», *Cardozo Law Review*, vol. 45, no. 2, 2023, pp. 351-403.

GREENLEAF, Graham, «Global Data Privacy Laws 2023: 162 National Laws and 20 Bills», *Privacy Laws and Business International Report*, vol. 181, no. 1, 2023, pp. 2-4. UNSW Law Research Paper No. 23-48, available at SSRN: https://ssrn.com/abstract=4426146

GREENLEAF, Graham, «Proposed US federal data privacy law offers strong protections but only to US residents», *Privacy Laws & Business International Report,* vol. 179, no. 1, 2022, pp. 3-7. UNSW Law Research Paper No. 22-50, available at SSRN: https://ssrn.com/abstract=4342518

GREENLEAF, Graham, « 'European' Data Privacy Standards Implemented in Laws Outside Europe», *Privacy Laws and Business International Report*, 2017, vol. 149, no. 1, pp. 21-23. UNSW Law Research Paper No. 18-2, available at SSRN: https://ssrn.com/abstract=3096314

JIMÉNEZ-GÓMEZ, Briseida Sofía, «Arbitraje sobre controversias de protección de datos en el acuerdo entre los Estados Unidos y la UE», *La Ley: Mediación y Arbitraje*, no. 21, 2024, pp. 1-45.

JIMÉNEZ-GÓMEZ, Briseida Sofía, «Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute», *Santa Clara Journal of International Law*, vol. 19, issue 2, 2021, pp. 1-45.

JURCYS, Paulius, CORRALES COMPAGNUCCI, Marcelo, FENWICK, Marc, «The future of international data transfers: Managing legal risk with a 'user held' data model», *Computer Law & Security Review*, vol. 46, 2022, Article 105691, HTTPS://DOI.ORG/10.1016/J.CLSR.2022.105691

KOKOTT, Juliane, SOBOTTA, Christoph, «The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR», *International Data Privacy Law*, 2013, Vol. 3, No. 4, pp. 222-228.

KORFF, Douwe, «Korff on Kuner: Schrems II Re-Examined», *Data protection and digital competition*, (3.09.2020), https://www.ianbrown.tech/2020/09/03/korff-on-kuner-schrems-ii-re-examined/

KUNER, Cristopher, «Schrems II Re-Examined», *Verfassungsblog* (25.08.2020), https://verfassungsblog.de/schrems-ii-re-examined

KUNER, Cristopher, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013.

LENAERTS, Koen, «Limits on Limitations: The Essence of Fundamental Rights in the EU», *German Law Journal*, vol. 20, 2019, pp. 779–793.

MOEREL, Lokke, *Binding Corporate Rules*, Corporate Self-Regulation of Global Data Transfers, Oxford University Press, 2012.

NISSENBAUM, Helen, *Privacy in Context: Technology, Policy, and The Integrity of Social Life*, Stanford University Press, 2010.

NOJEIM, Greg, LORENZO PEREZ, Silvia, «Trump's Sacking of PCLOB Members Threatens Data Privacy», *Lawfare*, 31 January, 2025, available at https://www.lawfaremedia.org/article/trump-s-sacking-of-pclob-members-threatens-data-privacy

NOYB, «US Cloud soon illegal? Trump punches first hole in EU-US Data Deal», 23.01.2025, available at: https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal

NOYB, *European Commission gives EU-US data transfers third round at CJEU*, 10.07.2023, available at: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

ORTEGA GIMÉNEZ, Alfonso, «¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EE.UU.», *Cuadernos de Derecho Transnacional*, vol. 16, Nº 1, 2024, pp. 483-513.

PURTOVA, Nadezhda, *Property Rights in Personal Data, A European Perspective*, Alphen aan den Rijn, Wolter Kluwer, 2012.

REIDENBERG, Joel R., «Resolving Conflicting International Data Privacy Rules in Cyberspace», *Stan. L. Rev*., vol. 52, 1999-2000, p. 1315 y ss., p. 1318.

RUBINSTEIN, Ira, MARGULIES, Peter, «Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground», *Connecticut Law Review*, vol. 54, 2022, pp. 518-456.

SHEN, Lei, *et al*., «FTC Targets Algorithmic Discrimination in Settlement With Rite Aid», *Cooley*, 24.01.2024, https://cdp.cooley.com/ftc-targets-algorithmic-discrimination-in-settlement-with-rite-aid/

SOLOVE, Daniel J., KEATS CITRON, Danielle, «Standing and Privacy Harms: a critique of Transunion v. Ramirez», *Boston University Law Review Online*, vol. 101, 2021, pp. 62-71.

STUCKE, Maurice E., «Addresing Personal Data Collection as Unfair Methods of Competition», *Berkeley Technology Law Journal*, vol. 38, issue 2, 2023, pp. 717-795.

TRIFON, Tara L., KRESS, Lindsey E., «The Murky Waters of the CCPA's Private Right of Action: Real and Perceived Ambiguities Complicating Litigation», *Privacy & Cybersecurity Newsletter*, Nov. 2024, available at https://www.lockelord.com/newsandevents/publications/2020/11/the-murky-waters

VOSS, W. Gregory, «Transatlantic Data Transfer Compliance», *Boston University Journal of Sciences and Technology Law*, vol. 28, 2022, pp. 158-214.