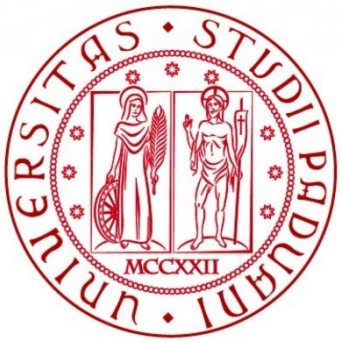

Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2024/2025

Surveillance and Privacy in EU-US Data Transfers: the role of U.S. Public Authorities under the New Regulatory Framework

Relatrice: Annalisa Volpato

Studente: Trolese Veronica

Abstract

This thesis aims to analyse the developments in cross-border data transfers between the European Union (EU) and the United States (U.S.), with particular focus on the role of U.S. authorities and their use and access of EU citizens' personal data under the new *Data Privacy Framework*. First, it provides an overview of the past agreements between the EU and the U.S. concerning data transfers, such as the Safe Harbour and the Privacy Shield frameworks, and their respective annulments following *Schrems I* and *Schrems II* rulings. Furthermore, the current *Data Privacy Framework* is analysed evaluating its effectiveness against surveillance practices by U.S. authorities. The thesis then shifts focus on U.S. laws, examining whether they overreach the EU privacy standards, potentially allowing illegal access to data subject to transfers, with particular emphasis on the role of U.S. authorities. Finally, future perspectives are discussed, considering potential regulatory developments and the broader implications for the protection of personal data in transatlantic relations.

Riassunto esteso in lingua italiana

Il presente elaborato si propone di analizzare l'evoluzione dei trasferimenti transfrontalieri di dati personali tra l'Unione Europea (UE) e gli Stati Uniti d'America (US), con particolare attenzione al ruolo delle autorità statunitensi e al loro utilizzo e accesso ai dati personali dei cittadini europei nell'ambito del nuovo *Data Privacy Framework*. In una prima parte, viene fornita una panoramica degli accordi precedenti tra UE e US in materia di trasferimento dei dati: il Safe Harbour e il successivo Privacy Shield, entrambi annullati dalla Corte di giustizia dell'Unione Europea nelle sentenze *Schrems I* (2015) e *Schrems II* (2020), per incompatibilità con gli standard di tutela europei, in particolare per la mancanza di tutele effettive contro la sorveglianza di massa. Successivamente, viene esaminato il contenuto e le novità introdotte dal vigente *Data Privacy Framework*, adottato nel 2023, valutandone l'efficacia alla luce delle modifiche normative introdotte dal governo statunitense, come l'Executive Order 14086 e l'istituzione del Data Protection Review Court. Un'ulteriore sezione dell'elaborato approfondisce la normativa americana vigente, in particolare il Foreign Intelligence Surveillance Act (FISA), analizzando se essa ecceda gli standard europei in materia di privacy. Vengono inoltre analizzate le autorità pubbliche statunitensi coinvolte nel funzionamento del Data Privacy Framework, come il Privacy and Civil Liberties Oversight Board (PCLOB), il quale svolge funzioni di supervisione e monitoraggio sulle attività di sorveglianza. Infine, vengono discusse le prospettive future, tra cui l'eventualità di un nuovo contenzioso dinanzi alla Corte di Giustizia (potenziale "Schrems III"), ipotesi resa ancor più concreta alla luce dei risultati della prima revisione annuale del Data Privacy Framework, che ha evidenziato alcune criticità residue. Si riflette, pertanto, sulla necessità di una cooperazione normativa più solida tra UE e US, che assicuri un livello elevato e sostanziale di tutela dei diritti fondamentali dei cittadini europei.

Contents

Introduction

In an era where data has become one of the most valuable resources for the economic and social growth of businesses and countries, cross-border data flows represent a great benefit. However, over the years, the increase in such flows has raised concerns about data protection and the need for adequate regulations; this is particularly true in relation to transfers between different jurisdictions such as the European Union (EU) and the United States (U.S.).

In 2018, the EU adopted the General Data Protection Regulation (GDPR), a comprehensive privacy law that outlines the conditions under which personal data of EU citizens must be handled.[1] At its core, European legislation is focused on safeguarding individual rights.[2] In contrast, the U.S. does not have a federal *omnibus* data protection law and prioritizes economic development, disregarding individual's rights.[3]

Following the invalidation of the *Privacy Shield framework* by the Court of Justice of the European Union (CGUE) in 2020, significant privacy concerns have emerged regarding the potential misuse of data by hand of the U.S. In response, the EU adopted a new adequacy decision, known as "*EU-US Data Privacy Framework*", aimed at ensuring greater compliance and establishing specific standards that organizations must adhere to.

[1] 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 L119
[2] Bradford Anu, *Digital Empires: The Global Battle to Regulate Technology* (New York, 2023, online edn, Oxford Academic, 21 Sept. 2023) accessed 13 June 2025, p.105-146
[3] ibid p.33-68

The purpose of this thesis is to assess whether the U.S. provides a level of protection for personal data, particularly in the context of government surveillance, that is considered adequate under EU law, with focus on the role of U.S. public authorities within the new transatlantic framework. This includes a thorough analysis of the U.S. legal framework governing data protection and its alignment with the new *EU-US Data Privacy Framework*. The investigation will also focus on the role of U.S. oversight authorities, emphasizing the limits on the access and use of data, as well as the redress mechanisms that must be in place to ensure compliance.

The first chapter outlines the history of data transfers between the U.S. and the EU, with particular reference to the *Schrems I* and *Schrems II* rulings and the correlated invalidation of the *Safe Harbour* and *Privacy Shield* decisions. The second chapter illustrates the key points of the new *Data Privacy Framework*, examining whether it addresses concerns related to U.S. authorities' access to data, with a particular focus on national security and surveillance practices. It also analyses U.S. laws that authorize the collection, access and use of personal data, such as the Foreign Intelligence Surveillance Act, with particular emphasis on Section 702, and Executive Order 12333. The chapter then describes the role of oversight authorities and current redress mechanisms. Finally, it discusses future critical perspectives and challenges.

1. Overview of the EU-US data transfer history

The first formal cross-border data transfer rules were set out by Directive 95/46/EC[4], also known as "Data Protection Directive", which was in force from 1995 to 2018. The key principle, enshrined in Article 25, provided that data could not be transferred to third countries unless the recipient country ensured an adequate level of protection. Absent thereof, the transfer of data could have only taken place in the presence of specific conditions laid down by Article 26. Article 28 also provided that each Member State should have had a supervisory authority with significant powers to ensure compliance its provisions.

The exponential increase of data value and the shift to a data-driven world generated the need to ensure stronger and more extensive protection of individuals' personal data. By 2018, the EU adopted the General Data Protection Regulation (GDPR), which fully replaced Directive 95/46/EC.

1.1. *Schrems I* and the annulment of the *Safe Harbour* Decision

In 2000, the EU adopted an adequacy decision under Article 25 of Directive 95/46/EC, known as "*Safe Harbour*",[5] and related FAQs issued by the U.S. Department of Commerce. This was the first formal agreement between the EU and the U.S. regulating cross-border transfers of personal data, establishing strict privacy standards for U.S. recipients. Among these were the Notice and Choice principles, which required individuals to be clearly informed on the collection, use and possible sharing of their personal data, as well as

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

[5] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215 [2000]

the option to opt out.[6] Additionally, U.S. companies had to ensure adequate Security and Data integrity to prevent data loss, damage or misuse. As last, individuals had the right to access to their personal information and, in order to ensure compliance with these principles, enforcement mechanisms had to be guaranteed.[7] U.S. companies had to self-certify to the U.S. Department of Commerce that they adhered to the Safe Harbour principles and had to carry out annual audits to verify compliance.

In June 2013, the stability of the Safe Harbour agreement was negatively affected by the so-called *Snowden* case, in which Edward Snowden, a former National Security Agency (NSA) intelligence contractor, disclosed secret information regarding the PRISM programme, a collaboration between the NSA and tech companies to access users' personal data[8]. The aim of the programme was to collect intelligence information for national security purposes. Following the revelation of mass surveillance programmes, which also affected EU citizens' personal data, the EU Commission raised concerns on U.S. surveillance practices and their impact on privacy rights, emphasizing the need to restore trust in data transfers between the EU and the U.S. through better transparency and greater commitment to the protection of fundamental rights by U.S. authorities.[9] The Commission underlined the importance of data flows in "*commercial exchanges across the Atlantic including for new growing digital businesses*"[10] and emphasized the need to strengthen the *Safe Harbour* scheme. Finally, the Commission found that a relevant number of certified

[6] ibid Annex 1
[7] ibid Annex 1
[8] John W. Rollins and Edward C Liu, *NSA Surveillance Leaks: Background and Issues for Congress* (2013) Congressional Research Service, p.1-21
[9] European Commission, Communication "*Restoring Trust in EU-US Data Flows*", COM(2013) 846 final.
[10] ibid point 1

companies did not comply with the Safe Harbour Principles[11] and that "*a number of legal bases under U.S. law allow large scale collection and processing of personal data* (…)".[12]

In the wake of Snowden's revelations, tensions increased and led to a legal dispute that highlighted the inadequacy of the Safe Harbor agreement: the *Schrems* case[13]. In June 2013, Maximilian Schrems, an Austrian lawyer and activist, filed a complaint to the Irish Data Protection Commissioner, asking to prohibit Facebook Ireland from transferring his personal data to the Facebook Inc. established in the United States. In the light of the acknowledgement of U.S. surveillance practices, Mr. Schrems argued that the U.S. did not ensure an adequate level of protection. However, the Commissioner maintained that he wasn't competent on the matter and rejected the complaint as unfounded.[14] Additionally, he believed that there was no evidence that Mr. Schrems' personal data had been accessed by the NSA. Thus, Mr. Schrems brought an action before the Irish High Court, which noted that the Safe Harbor agreement didn't guarantee an adequate level of protection and that surveillance practices constituted a violation of the EU Charter of Fundamental Rights, particularly Articles 7, 8 and 47. However, given the complexity of the legal matter, the High Court decided to refer the case to the CJEU for a preliminary ruling, asking whether national data protection authorities had the power to investigate and take action against data transfers subject to insufficient protection[15]. The Court ruled that the Safe Harbour Decision pursuant to Directive 95/46/EC "*does not*

[11] European Commission, Functioning of the Safe Harbour from the Perspective of EU citizens and Companies Established in the EU, COM(2013) 847 final, points 3-5, 8
[12] ibid point 7
[13] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 (Grand Chamber)
[14] ibid para 28-29
[15] ibid para 36

prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[16] Additionally, the Court upheld that the Decision didn't provide an adequate level of protection of EU citizens' personal data as required by Article 25 of Directive 95/46/EC, and U.S. laws didn't limit interference with fundamental rights.[17] Therefore, the CJEU declared Decision 2000/520/EC invalid.[18]

The *Schrems I* case was a landmark ruling that established that, in the balance between EU citizens' privacy rights and the interests requiring free movement of personal data, privacy protection cannot be compromised and must prevail.[19]

1.2. A new arrangement: The *Privacy Shield*

In July 2016, the EU Commission adopted Decision 2016/1250[20], also known as "EU-U.S. Privacy Shield", establishing that the U.S. ensures an adequate level of protection for the transfer of personal data from the EU to self-certified organisations in the U.S.[21] The Decision was based on the findings of the CJEU in the *Schrems I* ruling, which invalidated the previous Safe Harbour Agreement.

---

[16] *Schrems I*, Case C-362/14, 'Costs' point 1
[17] ibid para 98, 88
[18] ibid para 106
[19] Philipp Fischer, *Getting Privacy to a new Safe Harbour*. Comment on the CJEU judgment of 6 October 2015, Schrems v Data Protection Commissioner, 6 (2015) JIPITEC 229 para 1, point 13
[20] Commission Implementing Decision (EU) 2016/1250 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, OJ L 207 [2016]
[21] ibid para 13

The *Privacy Shield* introduced more detailed and robust privacy principles, such as the data integrity and purpose limitation principle which set specific requirements to limit data retention and usage.[22] With regard to the purpose limitation principle, there is a growing number of cases in which personal data, once collected, is subsequently used for purpose different from those for which it was originally gathered. This is particularly troubling when, for example, data collected for commercial purposes is later repurposed for entirely different objectives, such as law enforcement activities.[23] Additionally, the framework introduced the recourse, enforcement and liability principle, which required transparent privacy practices, effective remedies and independent oversight for individuals affected by an organisation's non-compliance.[24] The right of access was also strengthened through clearer limits on exceptions and stronger enforcement and redress options.[25]

Regarding the access and use of personal data by U.S. public authorities for national security purposes, the Commission, after thorough analysis, found that U.S. laws, such as Presidential Policy Directive 28 (PPD-28)[26], which imposed limitations on signal intelligence and bound the intelligence community, ensured adequate protection. Moreover, although Section 702 of the Foreign Intelligence Surveillance Act (FISA) provided a legal basis for surveillance programmes, it was determined that the searches were targeted, not broad in scope. The Commission established that the data collection had to be proportional and necessary, as any overreach would have constituted a

[22] ibid para 21
[23] Jasserand Catherine, *Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?*' (2018), European Data Protection Law Review, *4*(2), 152-167, p. 153
[24] ibid para 26
[25] ibid para 25
[26] Presidential Policy Directive 28, Signals Intelligence Activities (17 January 2014)

violation of privacy.[27]

The *Privacy Shield* framework also granted data subjects the right to lodge complaints, either to a self-certified organisation, an independent dispute resolution body designated by the organisation, national Data Protection Authorities, or to the Federal Trade Commission. Additionally, the Department of Commerce had a role in monitoring compliance with the Privacy Shield principles.[28]

Furthermore, the U.S. government created a new Ombudsperson Mechanism, allowing EU citizens to seek redress in case of misuse or violation of their personal data. This new body was an independent official from the U.S. State Department tasked with investigating individual complaints. As a result, the EU Commission assessed that the U.S. provided effective legal protection against intelligence agencies' access to personal data.[29] Lastly, it was established that the Commission would check periodically the adequacy of the level of protection ensured by the U.S. and would conduct an Annual Joint Review.[30]

The *EU-U.S. Privacy Shield* framework was a significant step forward for the legitimacy of data transfers, providing stronger protection and oversight mechanisms.[31] However, concerns regarding U.S. surveillance practices remained entrenched.[32]

---

[27] Decision 2016/1250 para 67-90
[28] ibid para 109-116
[29] ibid para 116-123
[30] ibid para 145-149
[31] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law* (2017), Georgetown Law Journal, Vol.106, No.1
[32] See, inter alia, Article 29 Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, WP 238 (13 April 2016)

1.3. Schrems II: the Privacy Shield invalidation

As a requirement of the Privacy Shield framework, the Commission carried out an annual review from 2017 to 2019. Overall, the reviews were generally positive, although they highlighted some areas for improvements, particularly concerning U.S. government surveillance.[33] This issue was not fully addressed, leading to *Schrems II* ruling by the CJEU in 2020.[34]

Following the *Schrems I* ruling, which invalidated the previous Safe Harbor decision, the case was referred back to the Irish Commissioner. In the course of further investigation, the Commissioner found that the majority of personal data was transferred from Facebook Ireland to Facebook Inc. under Standard Contractual Clauses (SCC) based on Decision 2010/87[35]. As a result, Mr. Schrems reformulated his complaint, arguing that U.S. surveillance programmes were incompatible with Articles 7, 8 and 47 of the EU Charter. Therefore, the SCC Decision could not lawfully justify the transfer of personal data to the U.S, leading Mr. Schrems to ask for the prohibition or suspension of his personal data being transferred to Facebook Inc. In July 2016, the Commissioner found that SCCs were binding only within the EU and not on U.S. authorities, thus conferring inappropriate protection to EU data subjects[36].

With regard to intelligence surveillance, it was found that non-U.S. persons were only covered by PPD-28, which still did not ensure a level of protection essentially equivalent to that guaranteed by Article 7 and 8 of the Charter.

[33] European Commission, Report from the Commission to the EU Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, COM(2019) 495 final

[34] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Lt. and Maximilian Schrems* [2020] ECLI:EU:C:2020:559 (Grand Chamber)

[35] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L39 [2010]

[36] High Court (Ireland), *Data Protection Commissioner v. Facebook Ireland Limited & Schrems*, [2016] IEHC 414

Additionally, concerning judicial protection, it appeared that the Privacy Shield Ombudsperson wasn't a tribunal in the sense of Article 47 of the Charter.[37]

On 4 May 2018, the High Court decided to refer specific questions to the CJEU for a preliminary ruling[38], referring to the provisions of Directive 95/46, which was set to be repealed 21 days later due to the entry into force of the General Data Protection Regulation (GDPR) on 25 May 2018. Considering that at the time, the CJEU had not yet issued a final decision, and by the time it did, the GDPR had already become effective, the questions at hand had to be answered in the light of the provisions of the GDPR.

Chapter V of the GDPR addresses the transfers of personal data to third countries or international organisations. Specifically, Article 45 provides that personal data can be transferred on the basis of an adequacy decision. Absent thereof, according to Article 46, the data transfer must be subject to appropriate safeguards, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs) and Codes of Conduct. In the absence of both an adequacy decision and appropriate safeguards, Article 49 outlines derogations for specific situations, such as the explicit consent of the data subject, the necessity of the performance of a contract and transfers related to legal claims.[39]

On the basis of the provisions of the GDPR, the CJEU clarified that the level of protection required by Article 46 of the GDPR on SCCs must be essentially equivalent to that guaranteed by the EU Charter.[40] Therefore, to assess the

[37] ibid para 64-65
[38] ibid para 68
[39] Artt. 45,46,49 GDPR
[40] *Schrems II*, Case C-311/18 para 105

correct level of protection, both the agreed contractual clauses and the most relevant aspects of the legal system of that third country in question must be taken into account, in particular those set out in Article 45.

Secondly, the Court ruled that the supervisory authority must suspend or prohibit a transfer to a third country under the SSCs adopted by the Commission if those clauses cannot be complied with in the third country and if compliance with Article 45 and 46 of the GDPR, as well as the EU Charter, cannot be ensured by other means.[41]

The Court then examined the validity of the SCC Decision, which had been questioned due to concerns over its territorial scope. Specifically, the decision did not refer to a third country, meaning that it could not bind U.S. authorities.[42] However, the Court found that the SCC Decision provided effective mechanisms to ensure adequate protection, such as a reference to compliance with the GDPR, the requirement for both the EU-based controller and the third country recipient to verify that the level of protection required by the GDPR was achieved and an obligation incumbent on the recipient to promptly inform the controller in case of incapacity to comply with the clauses. The examination had a positive outcome and no signs were found to support invalidation.[43]

Finally, the Court upheld concerns raised by the Commissioner regarding the lack of adequate protection of EU data subjects in relation to U.S. surveillance practices. The Court found that neither Section 702 of the Federal Intelligence Surveillance Act nor E.O. 12333 posed any effective legal limits on monitoring

[41] ibid para 113
[42] ibid para 123, 130-132
[43] ibid para 142, 148-149

programmes, thereby violating the principle of proportionality. According to this principle, such programmes should have only been implemented when strictly necessary.[44] Additionally, the Court noted the absence of redress mechanisms, as neither PPD-28 nor E.O. 12333 granted data subjects enforceable rights against U.S. authorities.[45]

Based on these findings, in 2020, the Court declared the EU-U.S. Privacy Shield Decision invalid. This decision left cross-border data transfers in a state of uncertainty, also leaving EU-U.S. businesses unsure about the continued effectiveness of SCCs. In fact, through SCCs, data controllers were burdened with the responsibility of becoming experts in third-country law, an almost impossible task, especially when dealing with non-democratic countries. They were, in effect, required to take on the role of the Commission in assessing whether a third country provided an adequate level of protection, turning the use of SCCs into “mini adequacy decisions”.[46]

[44] ibid para 178-180
[45] ibid para 181-184
[46] Kuner Christopher, *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation* (2020) European Law Blog, p.3-4

2. Decision (EU) 2023/1795: EU-US Transatlantic Data Privacy Framework

In the wake of the *Schrems II* ruling, tensions between the EU and the U.S. surrounding international data transfers significantly heightened, posing a threat to the stability of the digital economy.[47] Although data transfers could still take place through SCCs and other tools under Article 46 of the GDPR, the CJEU clarified in *Schrems II* ruling that, when necessary, it was incumbent on data exporters to adopt "supplementary measures" to ensure an adequate level of protection.[48]

Due to the lack of clarity regarding what these "supplementary measures" were, the European Data Protection Board (EDPB) adopted Recommendations 01/2020 addressing the issue[49]. These included various "technical measures" such as data pseudonymization, encryption or splitting the data between two or more independent processors located in different jurisdictions.[50]

These Recommendations were subsequently promoted by the EU Parliament in a Resolution[51], which also emphasized the need for meaningful reforms of U.S. surveillance laws and practices in light of a future renewed agreement on data transfers. The Parliament further expressed support for investments in European data storage tools to strengthen the EU's autonomy in data

[47] Murphy MH, *Assessing the implications of Schrems II for EU-US Data Flow*, International and Comparative Law Quarterly. 2022;71(1):245-262. doi:10.1017/S0020589321000348 p. 256
[48] *Schrems II,* Case C-311/18 para 131-133
[49] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted on 18 June 2021)
[50] ibid para 22-26
[51] 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 Maximilian Schrems ("Schrems II"), Case C311/18, (2020/2789(RSP))

management.[52]

In July 2023, following the issuance of Executive Order 14086[53] by President Biden, the EU Commission adopted Implementing Decision 2023/1795[54], known as “EU-US Data Privacy Framework” (DPF), pursuant to Article 45 of GDPR. This decision, the Commission’s third adequacy determination, established that the U.S. ensures an adequate level of protection for personal data subject to transfer, in line with EU privacy standards.

2.1. Objectives and main new aspects

The EU-US Data Privacy Framework (DPF) aims to establish a robust and effective mechanism for data transfers from the EU to the U.S., ensuring a level of protection for personal data that is essentially equivalent to that guaranteed under the GDPR and the Charter of Fundamental Right of the EU.

The entry into force of the GDPR in 2018 significantly impacted data protection not only within the EU, but also across borders. Due to the absence of a legal definition of “data transfer” in the GDPR, the EDPB, acting under Article 70(1)(e) GDPR, identified three cumulative criteria to qualify a processing as a transfer: 1) A controller or processor (“exporter”) is subject to the GDPR; 2) The exporter discloses by transmission or otherwise makes personal data available

[52] ibid para 12,14,26,31

[53] Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities (7 October 2022)

[54] Commission Implementing Decision EU 2023/1795 of 10 July 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, OJ L 231 [2023]

to another controller, joint controller or processor ("importer"); 3) The importer is in a third country or is an international organisation.[55]

These clarifications helped to provide more greater terminological precision, confirming that "*the EU-US DPF applies to organisations in the U.S. that qualify as controllers or processors*" and that "*U.S. processors must be contractually bound to act only on instructions from the EU controller*"[56].

As the former Privacy Shield framework, U.S. organisations must self-certify their adherence to the "EU-US Data Privacy Framework Principles" with the U.S. Department of Commerce (DoC), which is responsible for ensuring ongoing compliance of self-certified companies with the requirements.[57] This includes mechanisms for annual re-certification, compliance monitoring through 'spot checks' and the detection of false claims of participation.

The new Principles remain mainly unvaried since the Privacy Shield. Under the Purpose limitation and Choice principle, which provide that data should be processed lawfully, collected for a specific purpose and the individuals must be given the opportunity to opt out, particularly in the case of sensitive data, which requires express affirmative consent.[58] The principles of Data accuracy, Minimisation and Security require that personal data be adequate, relevant and not excessive, and protected through appropriate technical and organisational measures.[59]The Transparency principle ensures that data subjects are clearly

[55] EDPB, Guidelines 07/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (Adopted on 14 February 2023)
[56] Decision 2023/1795, para 12
[57] ibid para 9
[58] ibid para 13-15
[59] ibid para 20-24

informed about the main aspects of the processing.[60] The Access principle grants individuals the right to access their data, rectify or amend inaccuracies and request the erasure of data unlawfully processed, with organisations required to respond within a reasonable period of time.[61] Furthermore, the DPF introduced more severe restrictions on Onward Transfers, requiring a contract whenever U.S. certified organisations further transfer EU-origin data to third parties.[62] Lastly, the Recourse, Enforcement and Liability principle obliges organisations to adopt appropriate mechanisms to monitor compliance and to verify that their privacy policies are consistent with the DPF requirements.[63]

In addition, enforcement has become more stringent and a new redress mechanism has been introduced, which will further be discussed.

2.2. Access and use by U.S. public authorities for national security purposes

In the light of *Schrems II* ruling, the Commission determined that the U.S. had enacted adequate reforms, such as E.O. 14086[64], fulfilling the "essential equivalence" test. As a result, personal data can be legally transferred from the EU to U.S. certified organisations under the DPF. The EU Commission clarified that *"any limitation to the right to the protection of personal data must be provided for by law and the legal basis which permits the interference with such right must itself define the scope of the limitation to the exercise of the right concerned"[65].* Furthermore, it established that the legal basis must include

[60] ibid para 25-28
[61] ibid para 30-32
[62] ibid para 38
[63] ibid para 45
[64] E.O. 14086
[65] ibid para 89, line 1-3

"*clear and precise rules*"[66] that are *"legally binding and enforceable by individuals"*[67]. Indeed, data subjects must be able to bring a legal action before an independent tribunal.[68]

U.S. public authorities may collect and process personal data from certified organisations for national security purposes under a specific legal framework, which includes limitations and safeguards that need to be observed. The relevant legal framework includes the Foreign Intelligence Surveillance Act (FISA) and presidential Executive Order 12333 (E.O. 12333), both in force at the time of the Safe Harbor and Privacy Shield decisions. Additionally, Executive Order 14086 (E.O. 14086), issued by President Biden, largely replaces Presidential Policy Directive (PPD-28). It is important to note that E.O. 14086 is binding on the entire Intelligence Community, whose agencies are required to update their policies and procedures within a year in order to be in line with the new requirements. This verification is carried out by the Privacy and Civil Liberties Oversight Board (PCLOB).[69]

2.2.1. Section 702 FISA and the related E.O. 12333

The invalidation of both the Safe Harbour and the Privacy Shield was driven by concerns over U.S. surveillance practices. At the core of these concerns were two key instruments of U.S. intelligence law: FISA and E.O. 12333.

The FISA was enacted in 1978 in response to abuses of U.S. individuals' privacy by the U.S. government conducted in the name of national security

[66] ibid para 89, line 6
[67] ibid para 89, line 9
[68] ibid para 89, line 10
[69] ibid para 119-126

purposes.[70] This legislation sets out protocols for physical and electronic surveillance, as well as collection of foreign intelligence information against potential threats to national security, such as terrorist attacks.[71]

Particularly relevant in this context is Section 702 FISA, enacted in 2008 as an amendment to the original 1978 statute, which establishes a judicial proceeding to authorize a specific form of data collection. Specifically, an independent court may allow the government to order U.S. organisations to disclose data of specific non-U.S. individuals located outside the U.S.

The U.S. government believes that such transfers under Section 702 FISA are lawful in the light of the GDPR's "public interest" derogation under Article 49.[72] Furthermore, it asserts that this information is regularly shared with EU Member States in order to cooperate against national threats.[73]

Based on these considerations, the Commission concluded that signal intelligence collection of data transferred to U.S. certified organisations is subject to limitations and safeguards under Section 702 FISA.[74][75] In the presence of a court's order or existing "*exigent circumstances*"[75] determined by both, they may "*authorize jointly, for a period up to 1 year from the effective date of authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."*[76]

---

[70] James G. McAdams, III *Foreign Intelligence Surveillance Act (FISA): An Overview*, p. 1

[71] The Foreign Intelligence Surveillance Act of 1978 (FISA) 50 USC § 1801 et seq

[72] Article 49 (1)(d) GDPR

[73] U.S. Department of Commerce, Department of Justice, Office of the Director of National Intelligence, White paper, September 2020 – *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, p. 2-4

[74] Decision 2023/1795 para 142

[75] 50 U.S.C. 1881a. "Procedures for targeting certain persons outside the United States other than United States persons" (c)(2) line 2

[76] ibid para (a)

This acquisition must be conducted in accordance with specific targeting procedures in order to ensure it only involves individuals "*reasonably believed to be located outside the United States*"[77] and to "*prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.*"[78]

Additionally, minimization procedures must be applied in order to limit the acquisition and retention of non-publicly available information relating to U.S. citizens.[79] The framework also mandates that authorized acquisition must comply with the Fourth Amendment of the U.S. Constitution.[80]

However, as established in the ruling *United States vs. Verdugo-Urquidez*[81], it appears that this constitutional protection applies only to individuals "*who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community*"[82]. Therefore, based on the interpretation in *United States v. Verdugo-Urquidez*, EU citizens are not protected under the Fourth Amendment.

The Foreign Intelligence Surveillance Court (FISC) is an independent tribunal responsible for reviewing certifications submitted annually by the Attorney General and the Director of National Intelligence for the collection of foreign

[77] ibid para (d)(1)(A)
[78] ibid para (d)(1)(B)
[79] ibid para (e)(1), section 1801 (h)
[80] Fourth Amendment of the U.S. Constitution, which reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[81] *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990)
[82] ibid para 265

intelligence information under Section 702 FISA. This includes the assessment of targeting and minimization procedures to ensure compliance with the requirements of FISA.[83]

One of the main concerns that emerged in the *Schrems II* ruling was whether the FISC adequately supervises the targeting of individuals. Following a review of U.S. law, it was found that the FISC is actively involved in overseeing the consistency of targeting procedures. As a matter of fact, the FISC must approve the certifications submitted by the Attorney General and the Director of National Intelligence, as well as the associated targeting and minimization procedures[84]. Moreover, the FISC evaluates in practice how the government implements these procedures and, if not satisfied, it can adopt binding remedial decisions.[85]

The National Security Agency (NSA) is responsible for carrying out targeting under Section 702 FISA. Analysts at the NSA are now required to provide a written explanation at the time of the targeting, facilitating the FISC's oversight.[86]

Unlike FISA, which permits the collection of personal data within the U.S., typically through service providers subject to U.S. jurisdiction, E.O. 12333 allows U.S. intelligence agencies to collect personal data outside the U.S. This may include personal data in transit between the EU and the U.S.[87]

E.O. 12333 is a broad presidential directive issued in 1981 with the objective of providing "*the necessary information on which to base decisions concerning*

[83] Decision 2023/1795 para 142-143
[84] U.S. White paper (Sept 2020) p. 7
[85] ibid p. 9
[86] ibid p. 8
[87] Decision 2023/1795 para 122

the conduct and development of foreign, defence and economic policy, and the protection of United States national interests from foreign security threats"[88]. Unlike FISA, it is not based on legislation passed by Congress and does not require judicial oversight, thereby undermining the right of EU data subjects to an effective remedy.[89]

Under E.O. 12333 *bulk collection*[90] may be conducted outside the U.S., but only when it is necessary to meet intelligence priorities and when targeted collection is not possible due to technical or operational reasons[91]. Even in such cases, this type of collection is subject to limitations and safeguards designed to prevent indiscriminate access to data.[92]

In this context, the *Schrems II* ruling highlighted that such collection "*which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without access being subject to any judicial review, does not, in any event, delimit sufficiently clear and precise manner the scope of such bulk collection of personal data*"[93]. However, the Court did not exclude this type of data collection, but rather upheld that such collection must take place lawfully.

Nevertheless, bulk data collection raises significant concerns, as it does not involve the acquisition of data from specific targets, but rather the mass collection of data to be scrutinized in a later stage.[94] This lack of limitations

[88] Executive Order 12333, United States Intelligence Activities (4 December 1981) – Part 1 1.1
[89] Art. 47 EU Charter
[90] Meaning the collection of large quantities of signals intelligence that is acquired without the use of discriminants, such as specific identifiers or selection terms.
[91] Decision 2016/1250 para 76
[92] Decision 2023/1795 para 141
[93] Decision 2023/1795 para 183
[94] Robbins Scott, *Bulk data collection, national security and ethics*, Political Science and Public Policy 2021, p.171

interferes with the necessity and proportionality principles enshrined in both the GDPR and in the EU Charter of Fundamental Rights. Consequently, surveillance programmes based on E.O. 12333 cannot be regarded as limited to what is strictly necessary.[95]

2.2.2. PPD-28 and E.O. 14086: impact on the protection of personal data

In 2014, following Edward Snowden's revelations on mass surveillance practices conducted by the U.S. government, PPD-28 was issued. The directive acknowledged that bulk collection could sometimes be necessary to identify threats; however, it placed limits on the use of data gathered through such methods.[96] Additionally, it introduced requirements aimed at safeguarding personal data regardless of an individual's nationality or place of residence.[97] Nevertheless, like E.O. 12333, PPD-28 did not grant judicially enforceable rights for private individuals who may have been subjected to unlawful surveillance.[98]

On October 2022, former U.S. President Biden adopted E.O. 14086[99], which largely replaced PPD-28 and introduced stronger limitations and safeguards for the collection and processing of personal data in the context of foreign intelligence. The order also established a new redress mechanism to address potential non-compliance with these new requirements.

The framework is of great relevance in the context of EU-US data transfers, as, unlike E.O. 12333 and FISA, it was introduced directly in response to the

[95] *Schrems II*, Case C-311/18 para 184
[96] PPD-28, Sec.2
[97] ibid Sec.4
[98] Linebaugh Chris D. and Liu Edward C., *Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield,* (Congressional Research Service, 2021) p.12
[99] E.O. 14086

invalidation of the Privacy Shield framework by the CJEU in the Schrems II ruling.

It is important to note that these new requirements introduced by E.O. 14086 supplement, rather than replace, the existing limitations provided by Section 702 FISA and E.O. 12333. Moreover, they are binding on the entire Intelligence Community, which is required to update its internal policies and procedures accordingly to ensure compliance.[100]

The new framework outlines twelve legitimate objectives and four prohibited objectives[101], some of which, as noted by the EDPB, appear to be quite general, creating uncertainties and undefined boundaries in relation to intelligence activities.[102]

These objectives must be pursued in light of concrete intelligence priorities, which have to undergo a specific process. Firstly, the Director of National Intelligence drafts a list of proposed priorities. Before these are submitted to the President for approval, each priority undergoes an assessment by the Civil Liberties Protection Officer (CLPO).[103] This evaluation ensures that the priorities are aligned with one or more legitimate objectives, do not reflect prohibited objectives and respect the privacy and civil liberties of individuals, regardless of their nationality.[104] Furthermore, the President may add other objectives "*in light of new national security imperatives*"[105] without the

[100] Decision 2023/1795 para 124-126
[101] E.O. 14086 Sec. 2 (b) (i,ii)
[102] EDBP, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (Adopted on 28 February 2023) para 115
[103] E.O. 14086, Sec. 2 (a)(iii)(A)
[104] Decision 2023/1795 para 135
[105] E.O. 14086, Sec. 2(b)((i)(B)

obligation to make them publicly available if doing so would pose a risk to national security. This lack of transparency applies not only to the general public but also to foreign governments and institutions, including the EU.

In addition, E.O. 14086 mandates that data collection activities strictly adhere to the principles of necessity and proportionality, as foreseen in the CJEU *Schrems II* ruling. As a matter of fact, E.O. 14086 establishes that signal intelligence activities may only be conducted "*following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority"*[106] and such activities must be carried out "*to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized*"[107]. This means that intelligence priorities must be balanced against the potential impact on individual's privacy. The framework notes that when collection is deemed necessary, it must be "*tailored as feasible*"[108] and must note negatively and disproportionately impact on constitutional rights and privacy freedoms.

It must be noted that bulk collection is allowed solely when targeted collection is not practicable, and when carried out outside the U.S., E.O. 14086 provides with additional safeguards.[109]

Despite these developments, the EDBP expressed concerns regarding the lack of independent prior authorisation, the absence of strict retention rules, the

[106] ibid Sec. 2(a)(ii)(A)
[107] ibid Sec. 2(a)(ii)(B)
[108] ibid Sec. 2(c)(i)(B)
[109] ibid para 141

possibility of temporary bulk collection, and insufficient safeguards concerning the dissemination of bulk-collected data.[110]

According to the EU Parliament resolution of May 2023, E.O. 14086 "*provides for significant improvements aimed at ensuring that these principles are essentially equivalent under EU law*"[111]. However, the resolution also notes that the definition and interpretation of these principles under E.O. 14086 are not fully aligned with EU law nor the standards established by the CJEU.

2.3. Access and use by U.S. public authorities for criminal law enforcement purposes

As regards the collection of personal data for criminal law enforcement purposes, the applicable procedures extend to all U.S. organisations, regardless of whether they are certified under the DPF or not. The limitations and safeguards are intended to protect individual's personal data, regardless of their nationality or place of residence.[112]

U.S. federal prosecutors and investigative agents may access personal data subject to transfer under the DPF through several mechanisms. Firstly, in the presence of a judicial warrant, authorities may carry out searches or seizures, including of electronically stored information. To issue such warrant, there must be a "probable cause" to believe that items related to a crime are located in a certain place.[113]

[110] EDBP, Opinion 5/2023, para 140-165
[111] European Parliament, Resolution of 11 May 2023 on the adequacy of the protection afforded by the EUUS Data Privacy Framework (2023/2501(RSP)) para 2
[112] Decision 2023/1795 para 91
[113] ibid para 92

Secondly, when investigating certain serious crimes, such as capital or infamous crimes, a grand jury may be requested to issue a subpoena[114], usually initiated by a federal prosecutor[115]. Such subpoena must be reasonable, not excessive and relevant to the investigation. [116] Other administrative subpoenas may also be issued to access data held by U.S. companies for public interest purposes.[117]

Additionally, U.S. law provides several legal bases for accessing communications data. Specifically, a court may authorize "*the collection of realtime, non-content dialling, routing, addressing and signalling information about a phone number or e-mail*"[118], only if the information is likely to be relevant and if the suspect's identity is priorly defined.

Furthermore, access to data held by internet service providers, telephone companies or similar entities for law enforcement purposes may be authorised by the Stored Communications Act (SCA). In order to access the stored content of electronic communications, criminal law enforcement authorities must typically obtain a warrant from a judge[119]

Lastly, a judge may authorize real time communication interceptions if "*there is a probable cause to believe that the wiretap or electronic interception will*

[114] ibid Annex VI p. 104
[115] Fifth Amendment to the U.S. Constitution – "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury"
[116] Decision 2023/1795 para 93
[117] ibid para 94
[118] ibid para 95
[119] ibid para 96

produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from the prosecution".[120]

In general, the EDPB recognizes that access to data for law enforcement purposes may be seen as seeking a legitimate objective.[121] Overall, the EDPB acknowledged that the U.S. system of law enforcement broadly aligns with the principles of necessity and proportionality enshrined in the EU Charter.[122]

However, the EDPB also highlights that not all procedures require a prior court intervention for individual collection measures before the usage, even though the majority of them presuppose it.[123] It is important to note that when the warrant requirement is not applicable, the Fourth Amendment[124] provides with a "reasonableness" test, aimed at ensuring that "*the U.S. government does not have limitless, or arbitrary, power to seize private information*"[125]. Therefore, even in the absence of a judicial warrant, the government must still comply with the standards of proportionality and legitimacy, thus ensuring a minimal threshold of legal protection.

[120] ibid para 98
[121] EDBP, Opinion 5/2023, para 83
[122] ibid para 89
[123] ibid para 90
[124] Fourth Amendment to the U.S. Constitution
[125] Decision 2023/1795 Annex VI

2.4. Oversight and enforcement: the crucial role of the FTC

The DPF provides with strict oversight and enforcement mechanisms to ensure that U.S. companies comply with its principles and that any non-compliance is promptly dealt with.[126]

The Department of Commerce (DoC) is in charge of the effective administration and oversight of the DPF program. This organism maintains a publicly available a list of U.S. organisations that have self-certified under the DPF and pledged to uphold its principles.[127] In order to continue to receive personal data from the EU, organisations are required to annually re-certify their adherence to the DPF.[128]

First, the DoC verifies that organisations fulfil the self-certification requirements, including that their privacy policies contain the necessary information as required by the Notice Principle. In the context of re-certification, the DoC carries out multiple checks, including "*to verify whether organisations' privacy policies contain a hyperlink to the correct complaint form on the website of the relevant dispute resolution mechanism*".[129]

The DoC also regularly monitors compliance with the principles through 'spot checks' of a random sample of organisations, as well as targeted checks when specific compliance concerns are raised.[130] When valid evidence of an organisation non-compliance emerges, the DoC requires the organisation to fill out and submit a detailed questionnaire. Failure to timely reply may lead to the

[126] Decision 2023/1795 para 47
[127] ibid Annex III pg. 82
[128] ibid para 49
[129] ibid para 50
[130] ibid para 53

referral of the organisation to the FTC or the DoT, both in charge of enforcement procedures. [131]

Moreover, the DoC identifies and addresses any false claims of participation by organisations which are either no longer part of the DPF list or have not been certified, both *ex officio* as well as on the basis of complaints from DPAs. In such cases, the Department verifies that fraudulent organisations remove any references to the DPF in their privacy policies that suggest their participation in the framework. Such references will be detected by the DoC e.g. through internet searches. In case of non-removal, the DoC may notify the organisations of a potential referral to the FTC/DoT.[132]

Regarding enforcement, both the Federal Trade Commission (FTC) and the Department of Transport (DoT) detain investigatory and enforcement powers to secure effective compliance with the DPF.

A crucial role is played by the FTC, an independent authority which enforces compliance through administrative or federal court orders to impose temporary or permanent injunctions, and other legal remedies. If organisations fail to comply, the FTC may pursue civil penalties and other corrective measures. To ensure transparency, the FTC keeps an online list of organisations subject to enforcement actions or court orders related to the DPF.[133]

[131] ibid para 54
[132] ibid para 53-57
[133] ibid para 59-63

The DoT, on the other hand, holds exclusive authority over airline privacy practices and shares jurisdiction with the FTC regarding the privacy practices of ticket agents involved in air travel sales.[134]

With respect to access and use of personal data for national security purposes, U.S. law provides with different bodies who are in charge of the supervision of U.S. intelligence activities and that can be categorized in internal and external.

Under E.O. 14086, each intelligence agency must appoint senior oversight and compliance officials, including Privacy and Civil Liberties Officers and Inspectors General, who are responsible for conducting period oversight of intelligence activities.[135]

Privacy and Civil Liberties Officers are in charge of the oversight of procedures to guarantee that the agency appropriately take privacy and civil liberties into account, and has established adequate mechanisms to handle complaints. They regularly submit reports to Congress and the PCLOB.[136]

Each agency also has an independent Inspector General responsible for the supervision of foreign intelligence practices. These entities have access to all information necessary to ensure compliance and can refer potential criminal violations for prosecution.[137] Overall, the EDPB acknowledges that Inspectors General detain broad investigative powers. However, these powers are not binding, particularly when making recommendations for corrective measures to

[134] Decision 2023/1795 para 64
[135] ibid para 161
[136] ibid para 164
[137] ibid para 165

the heads of the respective agencies. Nevertheless, the EDPB established that there are adequate internal supervisory mechanisms.[138]

Additionally, the Intelligence Oversight Board (IOB), which is part of the President's Intelligence Advisory Board (PIAB), ensures that U.S. intelligence agencies operate within the bounds of the Constitution and all applicable laws.

A particularly relevant oversight body is the PCLOB, which is tasked with overseeing counterterrorism policies and their execution, with a focus on safeguarding privacy and civil liberties. This organism is also responsible for overseeing the implementation of E.O. 14086. When revising their internal policies and procedures, intelligence agencies must consult the PCLOB, which will assess whether the revised policies align with the new standards.[139]

The EDPB considers the PCLOB as a credible and autonomous entity, "*whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been a particularly helpful source to understand the functioning of the various surveillance programs, to be an essential element of the oversight structure*".[140]

Overall, the Intelligence Community appears to be actively engaged in several initiatives aimed at enhancing transparency in the conduct of foreign intelligence activities.[141]

The role of these U.S. public authorities is crucial to the practical enforcement and accountability of the DPF. Their structure, powers, and degree of

[138] EDBP, Opinion 5/2023, para 190, 193
[139] Decision 2023/1795 para 166-167
[140] EDBP, Opinion 5/2023, para 201
[141] Decision 2023/1795 para 172

independence serve as an indicator of whether the commitments made under the DPF can be effectively implemented. Since this thesis aims to investigate the role of U.S. public authorities in the context of EU-U.S. data transfers, understanding the function of each institution is essential to assess both the robustness and the legitimacy of the new framework.

2.5. Redress mechanisms: DPRC and Ombudsperson mechanism

As established in Article 47 (2) CFR[142] and to guarantee an adequate level of protection, effective administrative and judicial remedies should be made available data subjects. In line with the Recourse, Enforcement and Liability Principle, organisations need to ensure that individuals affected by noncompliance have access to effective recourse mechanisms, enabling them to file complaints and have them properly addressed.[143]

Organisations may fulfil their redress obligations through independent mechanisms established either in the EU or the U.S., including independent alternative dispute resolution bodies or private-sector developed privacy programs. In this regard, individuals are provided with several avenues to enforce their rights and lodge complaints.

Firstly, data subjects may file a complaint with DPF organisations, who must include in their privacy policy a contact point and respond within 45 days.[144] Secondly, individuals may contact the independent dispute resolution body appointed by the organisation. Such remedy is subject to oversight by the DoC

[142] Article 47 (2) ECHR – "Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law."
[143] Decision 2023/1795 para 66
[144] ibid para 69

and the FTC.[145] Moreover, data subjects may bring a complaint with their national DPA. This mechanism requires the organisations' cooperation, which is facilitated through a dedicated contact point appointed by the DoC and the FTC.[146]

The DoC has committed to reviewing and making diligent efforts to address violations of the DPF principles. In case of persistent non-compliance, the DoC has the authority to remove the organisation from the DPF list. It is important to note that an organisation must fall under the jurisdiction of U.S. authorities, particularly the FTC, to ensure enforcement capability. If none of the above redress mechanisms resolve the complaint, the data subjects have the right to invoke binding arbitration by the EU-U.S. DPF Panel.[147]
Lastly, U.S. law offers further redress avenues.[148]

E.O. 14086 introduced a groundbreaking new recourse mechanism for complaints from EU data subjects related to U.S. signal intelligence activities, the CLOP-DPRC.[149] Unlike ordinary U.S. court proceedings, which require an individual to prove its damaged position - a standard greatly undermined due to the lack of notification in surveillance cases - this new mechanism allows individuals to file complaints without the need to demonstrate that their data was actually subject to surveillance.[150]

[145] ibid para 70
[146] ibid para 73-74
[147] ibid para 78-81
[148] ibid para 86
[149] E.O. 14086, Sec. 3
[150] EDBP, Opinion 5/2023, para 214-215

To initiate this process, an EU data subject must submit a complaint to their national DPA, which will verify whether it meets the necessary requirements and forward it to the newly established two-layered redress mechanism.

First, the Civil Liberties Protection Officer (CLPO) within Office of the Director of National Intelligence (ODNI) carries out the initial investigation.[151] The CLPO can access the necessary information and may be assisted Privacy and Civil Liberties Officers'. The ODNI CLPO mainly assesses whether a breach of applicable U.S. law has taken place and, if so, determines the appropriate remedial measures. Through the course of the review, the ODNI CLPO must maintain appropriate documentation, as well as produce a classified decision.[152] Such decision is binding on the intelligence agencies involved.[153]

Upon conclusion, the ODNI CLOP, via the DPA, informs the complainant that "*the review either did not identify any covered violations or the ODNI CLPO issued a determination requiring appropriate remediation*".[154]

If unsatisfied, the complainant, or the Intelligence community, may appeal the ODNI CLOP's decision to the Data Protection Review Court.

The DPRC is an autonomous tribunal in charge of impartially reviewing the ODNI CLPO's decision, as well as conducting its own investigation. It is composed of three panels, each of which is assisted by a Special Advocate, whose role consists of representing the complainant's interests. The DPRC has

[151] E.O. 14086, Sec. 3(c)
[152] ibid Sec.3 (c)(i)(F)(G)
[153] ibid Sec.3 (ii)
[154] ibid Sec.3 (c)((i)((E)(1)

full access to necessary information, which may be facilitated by the CLPO, who is obliged to cooperate.

The DPRC is required to adopt its decision in a written form on the basis of the majority of votes.[155] Unlike the previous Ombudsperson mechanism, the DPRC's decision is totally binding and, in case it results in a violation of the rules, it provides with appropriate remediation, such as the deletion of unlawfully collected data.[156] To this end, the EDPB notes that some uncertainty remains in determining what constitutes "appropriate remediation", and consideration should be given to "*the ways that a violation of the kind identified have customarily been addressed*"[157]. However, the precise meaning of this formulation remains unclear.[158]

Given that the DPRC's decisions are final and not subject to appeal, its functioning is subject to annual review conducted by the PCLOB. This review assesses whether the decision was taken in a reasonable period of time, if the access to all necessary information was granted, if E.O. 14086 safeguards were complied with, and whether the Intelligence Community adhered to such decision. The PCLOB will produce a report, as well as making a public certification of the consistency of the complaints with E.O. 14086 requirements.[159]

Overall, the EDPB welcomes the creation of a dedicated redress mechanism under E.O. 14086 to address and resolve complaints from non-US individuals regarding U.S. signal intelligence activities. It particularly supports the DPRC's

[155] Decision 2023/1795 para 185-191
[156] ibid para 191
[157] E.O. 14086, Sec.4(a)
[158] EDBP, Opinion 5/2023, para 232
[159] ibid para 194

legal basis in E.O. 14086, noting that this provides sufficient legal standing, as long as it is ensured with independence in practice. As a matter of fact, the previous Ombudsperson mechanism was criticized for lacking independence, as it was designated by and required to report to the Secretary of State, and had no protection for dismissal.

The DPRC addresses these issues by providing guarantees in relation to the designation and dismissal of its judges, strengthening its independence. Nevertheless, the EDPB notes that such independence must be verified also in practice.[160]

Finally, the EBPB welcomes the removal of any standing requirement under the new redress mechanism, considering it a major improvement. However, it points out that although non-US data subjects can technically go to ordinary U.S. courts, such courts require standing, and it is unclear how E.O. 14086 could practically apply. Therefore, the EDPB highlights the need to monitor such aspect in future reviews.[161]

2.6. Critical perspectives and challenges: Schrems III?

Although the formal entry into force of the EU-U.S. DPF, significant issues remain, many of which echo the deficiencies that led to the invalidation of its predecessors. The first periodic review[162] of the framework, published by the

[160] EDBP, Opinion 5/2023, para 217-224
[161] ibid para 235-237
[162] European Commission, Report from the Commission to the European Parliament and the Council on the first periodic review of the function of the adequacy decision on the EU-U.S. Data Privacy Framework COM(2024) 451 final

EU Commission, and the related EDPB Opinion,[163] provide both a general update and a thorough evaluation of the DPF's future sustainability.

One of the core weaknesses highlighted by both institutions is the limited awareness and use of available redress mechanisms.[164] In fact, the very low number of complaints filed suggests that individuals are either unaware of their rights or do not consider the mechanism effective. Although several awareness campaigns have been conducted by the DoC, the EDPB and the EU Commission, these efforts appear insufficient, raising doubts on the effective accessibility of the DPF for data subjects.

Furthermore, although the DoC has made technical improvements, such as implementing automated tools for compliance detection, the EDPB rightly warns that such automation can't substitute individual investigations.[165] Indeed, considering that automated tools operate in a generalized and standardized manner, they risk weakening the more individualized dimension of enforcement, thus affecting the effectiveness and accuracy of oversight activities.

With regard to the implementation of E.O. 14086, it appears that practical implementation and related verification of its effectiveness are still lacking. While intelligence agencies have developed new policies and undergone training, the EU Commission calls for concrete examples of how the order is

[163] EDPB, 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 (Adopted on 4 November 2024)
[164] Commission Review COM(2024) 451 final p.7
[165] EDPB, Report (4 November 2024), para 8

being applied in practice. In this respect, the role of the PCLOB in monitoring application is promising but still remains untested.[166]

A particularly relevant development is the re-authorisation of Section 702 FISA through the Reforming Intelligence and Securing America Act (RISAA), passed by Congress in April 2024. While the prohibition of "abouts" collection and the expansion of the definition of "electronic communication service providers"[167] suggest progress, the EDPB calls for clarity, pointing out that vague legal terminology still characterizes the U.S. system and compromises trust in it.[168] Such an expansion of the definition may in fact increase the scope of potential surveillance, consequently raising concerns about compliance with the proportionality and necessity standards enshrined in EU law.

In addition, while the new DPRC redress mechanism appears to be a major improvement compared to the former Ombudsperson mechanism, it has yet to be tested in practice yet. The same applies to its effectiveness and independence.[169] In this context, the EDPB's concerns regarding the whole new framework underscore that legal architecture alone is insufficient and concrete evidence is needed to assess the effectiveness of such mechanisms.

Lastly, the EDPB highlights the importance of ensuring an adequate level of protection even with regard to governmental acquisition of personal data by U.S. intelligence agencies from commercial entities that do not fall within E.O. 14086.[170] This appears problematic, as it creates a blind spot in the

[166] Commission Review COM(2024) 451 final p.11-12
[167] which now includes "*any other service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications"*
[168] EDPB, Report (4 November 2024), para 44
[169] ibid para 55-56
[170] ibid para 69

framework's surveillance limitations and may ultimately undermine the adequacy assessment.

At present, a case is pending before the CJEU involving French politician Philippe Latombe. In 2023, Latombe challenged the DPF, requesting its annulment on the grounds that it does not ensure an adequate level of protection.[171] Although the proceedings are still ongoing, this complaint, alongside previous challenges to earlier frameworks, illustrates the complexity of this matter. It suggests that lasting stability in the field of transatlantic data flows remains difficult to achieve.

[171] Case T-553/23 R: *Latombe v Commission* (Order of the President of the General Court of 12 October 2023) OJ C/2023/1164

3. Conclusion

The history of data transfers between the EU and the U.S. reflects a longstanding unresolved tension between national security interests and the EU's fundamental right to data protection. With a particular focus on the new DPF, this thesis has demonstrated that the role of U.S. public authorities is not merely procedural, but deeply structural in shaping the durability of transatlantic data transfers.

As discussed, the DPF has introduced several innovations, most notably the establishment of the DPRC and a more defined oversight structure. Nevertheless, the effectiveness of these mechanisms depends largely on how U.S. public authorities enforce their mandates under instruments such as E.O. 14086 and Section 702 FISA, both of which continue to raise concerns. FISA, in particular, appears to offer only limited protection for non-U.S. individuals, who are not covered by the Fourth Amendment. Moreover, E.O. 12333 allows bulk data collection, which conflicts with the EU's standards of necessity and proportionality.

On paper, E.O. 14086 appears to provide a solid foundation for a more balanced framework. Nonetheless, certain provisions remain overly broad and the order still allows for temporary bulk collection, thereby posing a threat to the rights of EU data subjects. Furthermore, the effectiveness of this order is contingent upon its actual implementation, which, as highlighted in the first review of the DPF, remains limited.

Oversight and redress bodies such as the DPRC and the PCLOB have been established to ensure that U.S. intelligence practices align with the principles

of necessity and proportionality. However, ongoing concerns persist regarding their effective independence and transparency.

In May 2025, controversy arose after President Donald Trump unlawfully dismissed two democratic members from the PCLOB, raising significant concerns about the board's autonomy. However, a federal judge recently declared such dismissal unlawful, reinstating the removed judges.[172] This incident underlined the critical importance of the PCLOB's bipartisan structure as a safeguard against excessive presidential power and as a mechanism to ensure independent oversight of government surveillance. Without at least three sitting members, the PCLOB can't meet quorum requirements, effectively preventing it from starting new projects or issuing official reports, including reviews of the EU-US DPF.

Overall, relevant step forwards have been made since the beginning of EU-US negotiations on a legal framework for data transfers. Nevertheless, the major barrier to transatlantic data flows is, and will likely remain, the different approaches to data protection of the two parties. These differences stem not only from legal frameworks, but also from deeper structural and cultural roots: two political systems, with contrasting institutional models and diverging conceptions of individual's rights, as well as different principles and objectives. While the EU prioritizes preserving privacy, the U.S. advocates innovation and development.

In this context, the U.S. is currently investing time and resources in developing Artificial Intelligence (AI), which requires vast amounts of personal data, raising

[172] Case 1:25-cv-00542-RBW, *Travis LeBlanc v. United States Privacy and Civil Liberties Oversight Board* (D.D.C 2025

new concerns regarding data protection in data transfers. One of the most pressing issues is the lack of transparency characteristic of many AI systems. In cases of violation of data protection rights, it may be nearly impossible to identify the violation itself or to assess the scope and impact of such violation.[173] This concern extends to other countries such as China, which has repeatedly faced criticism by the EU data protection authorities for lack of compliance with the GDPR. An emblematic case is DeepSeek, a Chinese large language model recently subjected to an investigation by the Italian DPA due to concerns about the collection, storage and the potential for access by Chinese authorities.[174] These dynamics highlight the complexity of international data transfers and the differing value placed on personal data across jurisdictions.

[173] See, inter alia, Poscher Ralf, *Artificial Intelligence and the Right to Data Protection,* in: Voeneky S, Kellmeyer P, Mueller O, Burgard W, eds. The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives (Cambridge University Press; 2022) 281-289, II

[174] Garante per la protezione dei dati personali, Press release – AI: The Italian Data Protection Authority blocks DeepSeek, January 2025

Bibliography

Primary sources

1)Legislation

Binding instruments

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 L119 [2016] ELI: http://data.europa.eu/eli/reg/2016/679/oj

Directive 95/46/EC of the European Parliament and 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 L281 [1995] ELI: http://data.europa.eu/eli/dir/1995/46/oj

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L215 [2000] ELI: http://data.europa.eu/eli/dec/2000/520/oj

Commission Implementing Decision (EU) 2016/1250 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, OJ L207 [2016] ELI: http://data.europa.eu/eli/dec_impl/2016/1250/oj

Commission Implementing Decision EU 2023/1795 of 10 July 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, OJ L 231[2023] ELI: http://data.europa.eu/eli/dec_impl/2023/1795/oj

Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L39 [2010]
ELI: http://data.europa.eu/eli/dec/2010/87/oj

Presidential Policy Directive 28, Signals Intelligence Activities (17 January 2014) Presidential Policy Directive -- Signals Intelligence Activities | whitehouse.gov

Executive Order 12333, United States Intelligence Activities (4 December 1981) Executive Orders | National Archives

Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities (7 October 2022) https://www.federalregister.gov/d/2022-22531

The Foreign Intelligence Surveillance Act of 1978, 50 USC § 1801 et seq
The Foreign Intelligence Surveillance Act of 1978 (FISA) | Bureau of Justice Assistance

Non-binding instruments

European Commission, Communication, Restoring Trust in EU-US Data Flows, COM(2013) 846 final EUR-Lex - 52013DC0846 - EN - EUR-Lex

European Commission, Functioning of the Safe Harbour from the Perspective of EU citizens and Companies Established in the EU, COM(2013) 847 final
EUR-Lex - 52013DC0847 - EN - EUR-Lex

Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, WP 238, 13 April 2016
ARTICLE 29 DATA PROTECTION WORKING PARTY

European Commission, Report from the Commission to the EU Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, COM(2019) 495 final eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0495

EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted on 18 June 2021)
Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board

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 Maximilian Schrems ("Schrems II"), Case C-311/18, (2020/2789(RSP)) EUR-Lex - 52021IP0256 - EN - EUR-Lex

EDPB, Guidelines 07/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (Adopted on 14 February 2023) Guidelines 05/2021 on the Interplay between the application of Article 3 and the

provisions on international transfers as per Chapter V of the GDPR | European Data Protection Board

U.S. Department of Commerce, Department of Justice, Office of the Director of National Intelligence, White paper, September 2020 – Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II

EDBP, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (Adopted on 28 February 2023) Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework | European Data Protection Board

European Parliament, Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)) European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP))

European Commission, Report from the Commission to the European Parliament and the Council on the first periodic review of the function of the adequacy decision on the EU-U.S. Data Privacy Framework COM(2024) 451 final
eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0451

EDPB, 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 (Adopted on 4 November 2024) EDPB 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 | European Data Protection Board

Garante per la protezione dei dati personali, Press release – AI: The Italian Data Protection Authority blocks DeepSeek, January 2025 COMUNICATO STAMPA - Intelligenza artificiale: il Garante privacy blocca... - Garante Privacy

2)Cases

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 (Grand Chamber) EUR-Lex - 62014CJ0362 - EN - EUR-Lex

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Lt. and Maximilian Schrems* [2020] ECLI:EU:C:2020:559 (Grand Chamber) EUR-Lex - 62018CJ0311 - EN - EUR-Lex

High Court (Ireland), *Data Protection Commissioner v. Facebook Ireland Limited & Schrems*, [2016] IEHC 414 Judgments | The Courts Service of Ireland

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)
United States v. Verdugo-Urquidez | 494 U.S. 259 (1990) | Justia U.S. Supreme Court Center

Case T-553/23 R: *Latombe v Commission* (Order of the President of the General Court of 12 October 2023) OJ C/2023/1164, http://data.europa.eu/eli/C/2023/1164/oj

Case 1:25-cv-00542-RBW, *Travis LeBlanc v. United States Privacy and Civil Liberties Oversight Board,* (D.D.C 2025) gov.uscourts.dcd.277733.24.0.pdf

Secondary sources

Bradford Anu, *Digital Empires: The Global Battle to Regulate Technology* (New York, 2023, online edn, Oxford Academic, 21 Sept. 2023) accessed 13 June 2025
Digital Empires: The Global Battle to Regulate Technology | Oxford Academic

Fischer Philipp, 'Getting Privacy to a new Safe Harbour. Comment on the CJEU judgment of 6 October 2015, Schrems v Data Protection Commissioner', 6 (2015) *JIPITEC* 229
View of Getting Privacy to a new Safe Harbour. Comment on the CJEU Judgment of 6 October 2015, Schrems v Data Protection Commissioner

Jasserand Catherine, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?' (2018) 4(2) *European Data Protection Law Review*, 152 https://doi.org/10.21552/edpl/2018/2/6

Kuner Christopher, "The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation." (2020) *European Law Blog*
https://doi.org/10.21428/9885764c.aed20daf

Linebaugh Chris D. and Liu Edward C., *Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield* (Congressional Research Service, 2021) EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield

López González, J., 'Trade and cross-border data flows' (2021), *OECD Going Digital Toolkit Notes*, No. 11, OECD Publishing, Paris https://doi.org/10.1787/7bc12916-en.

McAdams James G., III *Foreign Intelligence Surveillance Act (FISA): An Overview* Microsoft Word - Foreign Intelligence Surveillance Act.doc

Murphy MH, 'Assessing the implications of Schrems II for EU-US Data Flow' (2022) *International and Comparative Law Quarterly*. 2022;71(1):245-262. doi:10.1017/S0020589321000348 ASSESSING THE IMPLICATIONS OF SCHREMS II FOR EU–US DATA FLOW | International & Comparative Law Quarterly | Cambridge Core

Poscher Ralf, 'Artificial Intelligence and the Right to Data Protection' in Voeneky S, Kellmeyer P, Mueller O, Burgard W, eds. *The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives* (Cambridge University Press 2022) 281 Artificial Intelligence and the Right to Data Protection (Chapter 16) - The Cambridge Handbook of Responsible Artificial Intelligence

Robbins Scott, 'Bulk data collection, national security and ethics', *Political Science and Public Policy* (2021) https://doi.org/10.4337/9781800373075.00020

Rollins John W. and Liu Edward C., '*NSA Surveillance Leaks: Background and Issues for Congress*' (2013) Congressional Research Service, p.1-21 https://www.congress.gov/crsproduct/R43134

Schwartz Paul M. & Peifer Karl-Nikolaus, 'Transatlantic Data Privacy Law' (2017), *Georgetown Law Journal*, 106 https://www.law.georgetown.edu/georgetown-law-journal/inprint/volume-106/volume-106-issue-1-november-2017/transatlantic-data-privacy-law/

Surguy Mark. *International E-Discovery : A Global Handbook of Law and Technology* (Global Law and Business, 2019)

Trump dismantles surveillance watchdog, triggering Europe's privacy PTSD – POLITICO

https://www.politico.eu/article/french-lawmaker-challenges-transatlantic-data-deal-beforeeu-court/