University of Zagreb

Faculty of Law

Patricio Marcos Petrić

THE IMPACT OF EU-U.S. DATA TRANSFERS ON DATA PROTECTION

SPECIALIST THESIS

Zagreb, 2024

University of Zagreb

Faculty of Law

Patricio Marcos Petrić

THE IMPACT OF EU-U.S. DATA TRANSFERS ON DATA PROTECTION

SPECIALIST THESIS

Supervisors: Melita Carević, PhD and Tihomir Katulić, PhD

Zagreb, 2024

Pravni fakultet

Patricio Marcos Petrić

UTJECAJ PRIJENOSA PODATAKA IZ EU-A U SAD NA ZAŠTITU OSOBNIH PODATAKA

SPECIJALISTIČKI RAD

Mentori: izv. prof. dr. sc. Melita Carević
i izv. prof. dr. sc. Tihomir Katulić

Zagreb, 2024

Summary

This work examines the complex challenges of transatlantic data transfers, focusing on personal data transfers from the European Union (EU) to the United States (U.S.) on the basis of adequacy decisions. EU data protection standards stipulate that personal data transferred to third countries based on adequacy decisions must enjoy essentially the same level of protection as that within the EU. Personal data transfers to the U.S. are especially challenging considering their lack of robust federal data protection legislation and permissive personal data processing practices for national security purposes. Revelations in 2013 regarding U.S. intelligence's bulk data collection practices increased the interest of the public within the EU, leading to the invalidation of the Safe Harbour and Privacy Shield adequacy decisions by the Court of Justice of the European Union.

Currently, the adequacy decision based on the EU-U.S. Data Privacy Framework serves as the primary mechanism for such transfers, but its compliance with EU law remains in question. Key concerns include the persistence of bulk data collection without adequate independent administrative and judicial oversight and inadequate redress mechanisms for EU data subjects. This work critically analyses these ongoing deficiencies within the current adequacy decision and the proposed American Data Privacy and Protection Act, highlighting necessary legislative reforms to align with EU adequacy standards. Without significant improvements to U.S. data protection legislation, EU data subjects will continue to face risks, and transatlantic data transfers are likely to be disrupted by recurrent challenges to adequacy decisions. This analysis underscores the need for enduring solutions to ensure data protection across these interconnected yet distinct legal landscapes.

Keywords: data protection, EU-US Data Privacy Framework, personal data transfers, adequacy decisions, data subjects' rights.

Sažetak

Ovaj rad istražuje složene izazove transatlantskih prijenosa podataka, s fokusom na prijenose osobnih podataka iz Europske unije (EU) u Sjedinjene Američke Države (SAD) na temelju odluka o primjerenosti. Standardi zaštite podataka EU-a propisuju da osobni podaci preneseni u treće zemlje na osnovi odluka o primjerenosti moraju uživati suštinski istu razinu zaštite kao i podaci unutar EU-a. Prijenosi osobnih podataka u SAD posebno su izazovni s obzirom na nedostatak sveobuhvatnog zakonodavstva o zaštiti podataka na saveznoj razini te permisivne prakse obrade osobnih podataka u svrhe nacionalne sigurnosti. Razotkrivanje masovnog prikupljanja podataka američke obavještajne zajednice u 2013. povećalo je interes javnosti unutar EU-a, što je dovelo do proglašenja odluka o primjerenosti "sigurne luke" (*Safe Harbour*) i " europsko-američkog sustava zaštite privatnosti " (*Privacy Shield*) nevaljanima od strane Suda Europske unije.

Trenutačno, odluka o primjerenosti temeljena na “okviru EU-a i SAD-a za privatnost podataka” (*EU-U.S. Data Privacy Framework*) glavni je mehanizam za takve prijenose, no usklađenost iste s pravom EU-a ostaje upitna. Ključne sporne točke uključuju nastavak masovnog prikupljanja podataka bez odgovarajućeg neovisnog administrativnog i sudskog nadzora te nedostatne mehanizme zaštite ispitanika iz EU-a. Ovaj rad kritički analizira te nedostatke kao i sporne točke predloženog Američkog zakona o pravima na privatnost, naglašavajući potrebne zakonodavne reforme za usklađivanje s pravom EU-a. Bez značajnih poboljšanja pravnog okvira u SAD-u, ispitanici iz EU-a će i dalje biti izloženi rizicima, a transatlantski prijenosi podataka vjerojatno će biti podložni ponovljenim osporavanjima odluka o primjerenosti. Ova analiza naglašava potrebu za trajnim rješenjima koja će osigurati zaštitu podataka unutar ovih međusobno povezanih, ali pravno različitih sustava.

Ključne riječi: zaštita osobnih podataka, *EU-US Data Privacy Framework*, prijenosi osobnih podataka, odluka o primjerenosti, prava ispitanika.

Contents

1. Introduction

For data protection professionals, the transfer of personal data to third countries represents a specific challenge, considering the conflicting situations that require entities to simultaneously comply with opposing legal frameworks, one from the jurisdiction of the data exporter and the other from the jurisdiction of the data importer. The personal data transfers from the European Union (EU) to the United States of America (U.S.) are not an exception, especially considering the strong geopolitical and economic connections between these jurisdictions. However, these links were affected after the global surveillance measures of the U.S. authorities that gathered data from individuals globally, including those from the EU, were unveiled in 2013. The unveiling of information about the practices of the U.S. authorities has significantly impacted awareness among individuals regarding the importance of protecting their personal data. This helped EU individuals increasingly recognise the added value of businesses that offer better data protection features. Data subjects and data protection activists have increased their complaints against businesses that do not meet EU legal requirements, and EU data protection regulators have ramped up their advisory and investigative activities on international data transfers. For more than ten years, I have been navigating this complex, cyclical, and changing landscape of data protection transfers from the EU to the U.S. and, in this work, I am analysing the past and the present of this landscape and providing a perspective of its future that most probably will not be able to escape from its cyclical history.

The history of personal data protection is inseparably linked to the protection of personal data transfers, an issue that is increasingly critical in our interconnected world. As global data flows become the backbone of many activities in modern societies, the right to data protection, as enshrined in EU legislation, extends beyond its borders. This right is safeguarded through specific mechanisms designed to facilitate the transfer of personal data to third countries, alongside a limited set of derogations for exceptional circumstances.

The transfer of personal data from the EU to the U.S. has relied on various mechanisms tailored to fit the U.S. legal framework and simultaneously ensure compliance with EU standards. These mechanisms have been established through direct negotiations between the European Commission and U.S. representatives, taking into account the unique aspects of the U.S. legal system—most notably, the absence of comprehensive federal data protection legislation governing the processing of personal data in both the public and private sectors, and the traditional preferred position of U.S. citizens concerning data processing by public authorities.

The first two major agreements—the Safe Harbour Adequacy Decision and the Privacy Shield Adequacy Decision—were invalidated by the Court of Justice of the European Union following complaints lodged by Mr Schrems, a well-known data protection activist. These invalidations occurred despite the European Commission's and data protection authorities' reluctance to suspend data transfers, even when non-compliance with EU data protection standards was evident. The deficiencies identified by the Court of Justice of the European Union were closely tied to the widespread intelligence programmes for bulk data collection revealed by Mr Edward Snowden in June 2013. Additionally, the lack of data protection rights for EU individuals whose data was transferred to the U.S., including the absence of independent oversight and judicial redress, played a key role in the decisions of the Court of Justice of the European Union.

In this work, we will analyse the similarities between the deficiencies identified by the Court of Justice of the European Union in the Safe Harbour and Privacy Shield adequacy decisions. By examining these initial mechanisms for data transfer from the EU to the U.S., we will pinpoint the weaknesses in the current data transfer framework, the EU-U.S. Data Privacy Framework Adequacy Decision, which could potentially lead to its invalidation. Specifically, we will analyse the bulk collection of personal data by U.S. authorities, a practice that is in principle prohibited under EU law. We will also scrutinise the flaws in the oversight mechanisms under the EU-U.S. Data Privacy Framework Adequacy Decision, which involves a combination of different bodies with certain oversight powers on the entities performing the processing of transferred personal data. Furthermore, we will assess whether the redress mechanism established under the current framework meets the criteria required under EU law, including the obligation to provide reasoned decisions to data subjects.

The bulk collection of personal data by U.S. authorities is a significant point of contention. The indiscriminate collection of data, as practised in some U.S. intelligence programmes, starkly contrasts with the EU data protection principles. This tension underscores the fundamental differences in the approach to data protection between the EU and the U.S., where national security often takes precedence over individuals' data protection rights. Oversight mechanisms are another critical area of concern. Effective oversight requires the establishment of independent bodies empowered to monitor compliance and enforce data protection standards, and we will analyse whether the multiple oversight bodies mentioned in the EU-U.S. Data Privacy Framework Adequacy Decision are aligned with the EU requirements. Redress mechanisms provide another layer of protection for data subjects, which was not effectively provided by the first two transferring frameworks. Under EU law, individuals have the right to

seek judicial redress if their data protection rights are violated. We will analyse the adequacy of the redress mechanism in the EU-U.S. Data Privacy Framework Adequacy Decision, particularly whether it offers EU citizens the same level of protection and judicial recourse as that available within the EU, including the right of data subjects to obtain reasoned decisions from the redress bodies.

Finally, we will review the most recent legislative developments at the federal level in the U.S., namely the proposed American Data Privacy and Protection Act. Although this bill aims to establish comprehensive data protection standards in the U.S., we will assess the key deficiencies it contains that impede it from meeting EU data protection standards. This assessment will indicate the necessary changes to the U.S. legal framework to ensure that personal data transferred from the EU to the U.S. maintains the same level of protection as that in the EU. Such a level of protection would support a stable adequacy decision, safeguarding EU individuals' data and providing legal certainty to entities importing and exporting data across the Atlantic.

2. The beginnings of data protection legislation in the EU

The data protection legislation in the EU started with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter: Directive 95/46/EC)[1]. In the second recital of the aforementioned directive, the interconnection between data processing systems, fundamental rights, and socio-economic development, including trade expansion, is remarked upon. That recital specifies that "data processing systems [need to] respect [individuals'] fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals"[2].

In order to ensure the protection of personal data, Directive 95/46/EC also regulated transfers of personal data to other countries, aiming to ensure that highly protective standards are attached to personal data during its entire lifecycle. Considering the economic strength of the EU, such an approach has had a significant impact on data protection rules globally, leading other jurisdictions to recognise the necessity of complying with the strict EU standards. Thus, it could be said that transfers of personal data have been impacted by the "Brussels effect"[3]. One of such areas is privacy protection in which the EU is perceived to set the stricter standard than other countries,72 especially the US. The default approach implemented by the Directive 95/46/EC was to restrict personal data transfers from EU Member States only to third countries that ensure an adequate level of protection[4]. Such adequate level of protection would be granted considering "the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country"[5].

[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, p. 31).
[2] *Ibid,* recital 2.
[3] Vrbljanac, D., "Personal Data Transfer to Third Countries – Disrupting the Even Flow?", Athens Journal of Law - Volume 4, Issue 4, 2018, available on https://www.athensjournals.gr/law/2018-4-4-4-Vrbljanac.pdf, p. 351.
[4] Article 25(1) of Directive 95/46/EC.
[5] *Ibid*, Article 25(2).

The same directive had given the authority to the European Commission to declare that a third country provides an adequate level of personal data protection "by reason of its domestic law or of the international commitments it has entered into"[6].

Following the Article 25(6) of the Directive 95/46/EC, the Commission adopted two decisions on the adequacy of certain transfers of personal data to the U.S.: in July 2000, the Safe Harbour Adequacy Decision[7], and, after it was invalidated by the Court of Justice of the European Union in October 2015, the Privacy Shield Adequacy Decision[8] in July 2016.

3. EU standards for adoption of adequacy decisions

The right to personal data protection is a right that follows the collected personal data during its entire lifecycle, including when such data is transferred to a third country, unless derogations for specific situations apply.

Our attention will be focused on the international personal data transfers performed on the basis of an adequacy decision. As specified in Article 45(1) of the General Data Protection Regulation[9], personal data transfers can be carried out to a third country or an international organisation where the European Commission has decided that the third country, territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection.
In greater detail that the one provided by Directive 95/46/EC, the General Data Protection Regulation in its Article 45(2), clarifies which elements must be especially considered when assessing whether a third country or international organisation provides an adequate level of protection. These elements are:

"(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation

[6] Article 25(6) of Directive 95/46/EC.
[7] 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 U.S. Department of Commerce (notified under document number C(2000) 2441)) (OJ 2000 L 215, p. 7).
[8] 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) (OJ 2016 L 207, p. 1).
[9] 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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data"[10].

Regarding the elements that should be assessed prior to recognising that a third country provides an adequate level of protection, the predecessor of the European Data Protection Board[11], the Article 29 Data Protection Working Party[12], in its Adequacy Referential, points out two relevant aspects for such assessment. The first aspect is the provisions themselves and the second aspect are the means for their effective application[13]. In line with the Adequacy Referential, a third country or international organisation that aims to be recognised as a provider of an adequate level of protection needs to ensure the existence of data protection principles, effective procedures, and enforcement in practice, which are substantially comparable to the requirements emerging from the Charter of Fundamental Rights of the European Union[14] (hereinafter: the Charter) and the General Data Protection Regulation.

[10] Article 45(2) of the General Data Protection Regulation.
[11] The European Data Protection Board is an EU body with legal personality established by Article 68 of the General Data Protection Regulation.
[12] The Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection, with tasks described in Article 30 of Directive 95/46/EC and Article 15 of 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).
[13] Adequacy Referential Adopted on 28 November 2017 as last Revised and Adopted on 6 February 2018, WP 254 rev.01, Article 29 Working Party, p. 3.
[14] Charter of Fundamental Rights of the European Union (OJ 2016 C 202, p. 389).

Furthermore, another piece of guidance to assess the elements is the Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted by the European Data Protection Board[15]. As specified in the paragraph 7 of the Recommendations, their objective was to provide "elements to examine, whether surveillance measures allowing access to personal data by public authorities in a third country, being national security agencies or law enforcement authorities, can be regarded as a justifiable interference or not"[16]. In essence, these Recommendations ask for checking the existence of clear, precise, and accessible rules on personal data processing, the respect for necessity and proportionality with regard to the legitimate objectives pursued, a functioning independent oversight mechanism, and effective remedies available to individuals[17].

Regarding the scope of the assessment of the law and practices in a third country, it is interesting that, while the General Data Protection Regulation stipulates that it does not apply to personal data processing activities that "fall outside the scope of Union law, such as activities concerning national security"[18], at the same time, it is necessary to assess the defence and national security laws of a third country prior to granting an adequacy decision, as described in Article 45(2)(a) of the aforementioned Regulation. It is important to clarify that exchanges of personal data between private parties and national security services are covered by EU legislation, while exchanges between national security services, or interception of data from exchanges between private parties without their consent or awareness, escape the scope of EU law[19].

Once these elements are assessed, the European Commission may decide that such a country, territory, sector within a third country, or international organisation ensures an adequate level of protection. The adequacy decision needs to be adopted as an implementing act of the European Commission in accordance with the examination procedure defined in Article 5 of Regulation (EU) 182/2011[20], which includes the necessity to obtain a positive opinion from the

[15] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures Adopted on 10 November 2020, European Data Protection Board.
[16] Paragraph 7 of the Recommendations 02/2020 on the European Essential Guarantees for surveillance measures Adopted on 10 November 2020, European Data Protection Board, p. 5.
[17] Paragraph 24 of the Recommendations 02/2020 on the European Essential Guarantees for surveillance measures Adopted on 10 November 2020, European Data Protection Board, p. 8.
[18] Recital 16 of the General Data Protection Regulation.
[19] Granmar C.G., „A reality check of the Schrems saga", Nordic Journal of European Law, Volume 4 No. 2, 2021, p. 57, available on https://ssrn.com/abstract=4000713.
[20] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ 2011 L 55, p. 13).

Member States. The process also includes the obligation to ask the European Data Protection Board for its opinion regarding the adequacy decisions, as defined in Article 70(1)(s) of the General Data Protection Regulation.

There is also the obligation, established in paragraphs 3, 4, and 5 of Article 45 of the General Data Protection Regulation, to periodically review the adopted adequacy decisions by taking into account all relevant developments in the third country or international organisation, including their continuous monitoring by the European Commission in order to identify any issues impacting the adopted adequacy decisions[21].

In case the European Commission collects information revealing that the data protection standards in a third country or international organisation with an adequate level of protection do not meet the EU law requirements, the European Commission can repeal, amend, or suspend the adequacy decision in question by adopting an implementing act.

4. The first framework enabling free transfers of personal data to the U.S.

There are significant differences in the approach to data protection between the EU and the U.S. According to Gao and Chen, there is a "conceptual gulf" between these two jurisdictions based on their perceptions of data protection and privacy. In the EU, these values are an integral part of its "legal culture of fundamental rights". In contrast, the authors describe personal data under the U.S. legal framework as a commodity that can be commercially exploited under limited restrictions[22].

One specific aspect of the U.S. data protection legal framework is the absence of a federal data protection law. Instead, this area is segmented across different federal laws that cover specific sectors, such as the Health Insurance Portability and Accountability Act. Additionally, within the U.S., state legislation varies, with several states having adopted their own data protection laws.

On one hand, the fragmented data protection legal context in the U.S. presents challenges. On the other hand, the increasing volume of data transfers resulting from the advancement of

[21] Article 45(3), (4) and (5) of the General Data Protection Regulation.
[22] Gao X., and Chen X., "Understanding the Evolution of Transatlantic Data Privacy Regimes: Ideas, Interests, and Institutions", Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24), Association for Computing Machinery, New York, USA, 2024, available on https://doi.org/10.1145/3655693.3655720, p. 51.

technologies, particularly internet technologies and cloud-based services, has made granting free data flows from the EU to the U.S. an ever-growing economic necessity, while simultaneously posing a legal challenge.

Generally, before adopting a decision confirming that a third country provides an adequate level of data protection, the European Commission assesses the data protection laws of that country. If the assessment is positive, it follows the procedure described in Article 31 of Directive 95/46/EC. However, in this case, more detailed negotiations and the establishment of a specific framework were necessary to address the legislative vacuum and fragmentation of data protection in the U.S.[23]

In that context, the EU and the U.S. agreed to implement a set of rules for data transfers to U.S. companies that self-certify their adherence to the Safe Harbor Privacy Principles issued by the U.S. Department of Commerce and listed in the Annex I to the Safe Harbor Adequacy Decision. The Safe Harbor Adequacy Decision stated that such self-certified organisations were subject to the "statutory powers of a government body" in the U.S. that was "empowered to investigate complaints and obtain relief against unfair or deceptive practices, as well as provide redress for individuals […] in cases of non-compliance" with the Safe Harbor Principles[24].

The self-certification process was explained in FAQ 6 of Annex II to the Safe Harbor Adequacy Decision. According to the information provided in that section, self-certification would be carried out via a letter that the organisation needed to send to the Department of Commerce (or its designee) containing the organisation's basic information. The mentioned department would then maintain a publicly available list of all self-certified organisations that have submitted such letters, with the obligation to perform the self-certification on an annual basis.

The Principles represent the core of the Safe Harbour Adequacy Decision. As stated in the Safe Harbour Adequacy Decision, "the Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive of

[23] Taylor M., *Transatlantic Jurisdictional Conflicts in Data Protection Law*, Cambridge University Press, 2023, p. 196, available on http://dx.doi.org/10.1017/9781108784818.
[24] Article 1(2)(b) of the Safe Harbour Adequacy Decision.

Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts"[25].

Within the provided wide limitations, the Safe Harbor Principles aim to ensure the transparency of processing (Notice), provide control over personal data through opt-in or opt-out mechanisms depending on the circumstances (Choice), maintain a continuous level of data protection aligned with the Principles (Onward Transfer), implement precautions to protect processed personal data (Security), process only the personal data that is relevant to achieve the intended purposes (Data Integrity), empower individuals to access, correct, amend, or delete their personal data (Access), and implement effective protections to ensure that self-certified organisations comply with their commitments under the Safe Harbor Principles. This includes individuals' rights to have recourse mechanisms available, procedures for monitoring compliance, remediation mechanisms, and effective sanctions (Enforcement).

Considering the specific circumstances regarding the fragmented U.S. legislation and the various uncertainties surrounding the Safe Harbor Principles that emerged during negotiations between the EU and the U.S., the European Commission has identified the access and further use of transferred personal data by U.S. authorities under different laws as a potential issue. This access imposes limitations on individuals' data protection rights that exceed what is necessary and proportionate in a democratic society. Consequently, the European Commission has sought and obtained additional clarifications from the U.S. Department of Commerce on legal authorisations (among other topics) in U.S. legislation. Specifically, the European Commission requested an explanation regarding "explicit authorizations" in U.S. law for the processing of personal data "in a manner inconsistent with the safe harbor principles"[26].

From the answers provided by the U.S. Department of Commerce and included in the Safe Harbor Adequacy Decision, it is clear that the Safe Harbor Principles issued by this department hold a lower level of significance than the laws within the U.S. legal hierarchy. More precisely the Department of Commerce has answered that "while the safe harbor principles are intended to bridge the differences between the U.S. and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. The limited exception from strict adherence to the safe harbor principles seeks to strike a balance to accommodate the legitimate interests on each side"[27]. And further explains that "the exception is limited to cases

[25] Annex I to the Safe Harbour Adequacy Decision.
[26] Annex IV to the Safe Harbour Adequacy Decision.
[27] Annex IV(B) to the Safe Harbour Adequacy Decision.

where there is an explicit authorization. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorize the particular conduct by safe harbor organizations. In other words, the exception would not apply where the law is silent. In addition, the exception would apply only if the explicit authorization conflicts with adherence to the safe harbor principles"[28].

The aforementioned hierarchisation and the clarifications provided by U.S. authorities highlight one of the key deficiencies of the U.S. data protection system in comparison with countries that have comprehensive data protection laws. In the U.S., there is a clear supremacy of rules adopted by lawmakers over the data protection standards defined by the Safe Harbor Principles. In contrast, in countries with established data protection laws, the processing of personal data is equally governed by data protection laws as well as any other applicable law.

The Safe Harbor Adequacy Decision does not specifically address national security or the oversight of personal data processing for national security purposes. The only reference to national security activities relates to the exceptions concerning adherence to the Safe Harbor Principles. The same applies to the oversight of data processing activities by law enforcement authorities; the only topic mentioned in the Safe Harbor Decision pertains to cooperation in cases involving overlapping jurisdictions between the Federal Trade Commission (the authority responsible for supervising compliance with the Safe Harbor Principles) and other law enforcement agencies.

Finally, although it is not directly related to the U.S. data protection framework, the European Commission introduced a set of conditions and restrictions in Article 3 of the Safe Harbor Adequacy Decision regarding the powers of EU Member States' data protection authorities to investigate claims related to the transfer of personal data within the scope of the Adequacy Decision. These restrictions, along with many other aspects of the Adequacy Decision, will be addressed by the Court of Justice of the European Union.

a. The impact of unveiling the U.S. surveillance practices

More than a decade after the adoption of the Safe Harbour Adequacy Decision, in June 2013, a U.S. citizen involved in U.S. surveillance activities, Mr Edward Snowden, revealed information about various confidential global surveillance programmes carried out by U.S. intelligence authorities. This revelation soon undermined the trust of the European public, including EU

[28] *Ibid*.

Member States and institutions, in U.S. surveillance activities and transatlantic personal data transfers. The details are well documented chronologically in a publication by the European Parliament, where it is stated that the unveiling process started on "June 5th when The Washington Post and The Guardian published a secret order made under s.215 of the PATRIOT Act requiring the Verizon telephone company to give the NSA details of all U.S. domestic and international phone calls, and 'on an ongoing basis'" [29]. The day after, the same newspapers exposed the existence of National Security Agency's (hereinafter: NSA) secret surveillance programme called PRISM, which was used to extract data from the main U.S. Internet companies. In the same publication it is stated that "by the end of the day a statement from Adm.Clapper (Director of NSA) officially acknowledged the PRISM programme and that it relied on powers under the FISA Amendment 2008 s.1881a/702"[30]. On June 9th Mr Edward Snowden declared that the information was unveiled by him[31].

Within that context, the European Commission issued a Communication titled "Rebuilding Trust in EU-U.S. Data Flows"[32] (hereinafter: Communication on Rebuilding Trust), which is based on the Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection[33] (hereinafter: Report from 2013).

The Report from 2013 states that "in June 2013, the existence of a number of U.S. surveillance programmes involving the largescale collection and processing of personal data was revealed. The programmes concern in particular the collection of personal data from U.S. internet and telecommunication service providers and the monitoring of data flows inside and outside the US. Given the central position of U.S. information and communications technology companies in the EU market, the transatlantic routing of electronic data flows, and the volume of data flows across the Atlantic, significant numbers of individuals in the EU are potentially affected

[29] Bowden C. et al., The U.S. surveillance programmes and their impact on EU citizens' fundamental rights, European Parliament, Directorate-General for Internal Policies of the Union, Publications Office, 2013, https://data.europa.eu/doi/10.2861/34622, page 13.
[30] *Ibid*.
[31] *Ibid*.
[32] Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-U.S. Data Flows (COM(2013) 846 final), available on https://eur-lex.europa.eu/resource.html?uri=cellar:4d874331-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF
[33] Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection of 27 November 2013, available on https://cdn.netzpolitik.org/wp-upload/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

by the U.S. programmes"[34]. In the introduction of the Communication on Rebuilding Trust, the European Commission indicates that "the EU, its Member States and European citizens have expressed deep concerns at revelations of large-scale U.S. intelligence collection programmes, in particular as regards the protection of personal data" and concludes that "mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable"[35].

A timeline provided in the Report from 2013 shows the political approach taken to reestablish the confidence between the EU and US. As explained there, at the "EU-US Justice and Home Affairs Ministerial Meeting in June 2013, and in letters to their US counterparts, Vice-President Reding and Commissioner Malmström expressed serious concerns regarding the impact of these programmes on the fundamental rights of individuals in the EU, particularly the fundamental right to protection of personal data. Clarifications were requested from the US authorities on a number of aspects, including the scope of the programmes, the volume of data collected, the existence of judicial and administrative oversight mechanisms and their availability to individuals in the EU, as well as the different levels of protection and procedural safeguards that apply to US and EU persons"[36]. As further exposed, soon after that ministerial meeting, an ad hoc EU-U.S. Working Group was established in July 2013 to clarify the facts about the U.S. surveillance programmes and their impact on fundamental rights in the EU and on the personal data of EU data subjects. Among the EU members of the EU-U.S. Working Group was the Chair of the Article 29 Working Party[37].

In the Communication on Rebuilding Trust, one of the expressed doubts was "whether the largescale collection and processing of personal information under U.S. surveillance programmes is necessary and proportionate to meet the interests of national security"[38]. The European Commission also pointed out the result of the analysis carried out by the ad hoc EU-U.S. Working Group, where it is confirmed that "EU citizens do not enjoy the same rights and procedural safeguards as Americans"[39].

Based on the information gathered by the ad hoc EU-U.S. Working Group, the European Commission in its Communication on Rebuilding Trust confirmed that "the reach of these

[34] *Ibid*, p. 2.
[35] Communication on Rebuilding Trust, p. 2.
[36] Report from 2013, p. 2.
[37] *Ibid*.
[38] Communication on Rebuilding Trust, p. 4.
[39] *Ibid*.

surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement. The personal data of EU citizens sent to the U.S. under the Safe Harbour may be accessed and further processed by U.S. authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the U.S. internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme"[40]. That communication also severely criticised the gaps in the Safe Harbour Adequacy Decision and indirectly threatened when mentioning the European Commission's own power "to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection", adding that it can "reverse, suspend or limit the scope of the decision as well as adapt the decision at any time in the light of experience with its implementation"[41].

However, in addition to mentioning the strictest solutions—such as revocation, suspension, or limitation of the Safe Harbour Adequacy Decision—the European Commission has attempted to balance the necessity of protecting the fundamental right to personal data protection with the need to maintain fruitful business relations with the U.S. Consequently, while the European Commission acknowledged that the *current implementation of Safe Harbour cannot be maintained*, it also warned of the negative impact on business if the Safe Harbour Adequacy Decision were revoked. Ultimately, it concluded by supporting the option of implementing a balanced approach aimed at strengthening the Safe Harbour framework[42]. Essentially, the European Commission proposed to: (1) request that the U.S. administration refrain from accessing personal data held by private entities in the EU outside of formal cooperation channels, such as Mutual Legal Assistance agreements and sectoral EU-U.S. agreements, except in clearly defined, exceptional, and judicially reviewable situations; and (2) extend the safeguards available to U.S. citizens and residents to EU citizens who are not resident in the U.S.[43]

[40] *Ibid*.
[41] *Ibid*, p. 7.
[42] *Ibid*.
[43] *Ibid*, p. 10.

Along with the Communication on Rebuilding Trust, the European Commission issued the Communication on the Functioning of Safe Harbour[44]. Considering the concerns expressed in the Report from 2013, and in line with the Communication on Rebuilding Trust, in its introduction the European Commission emphasised the need to review the transfers of personal data to the U.S. based on the Safe Harbour Adequacy Decision due to the exponential growth in data flows from the EU to the U.S. and the revealed U.S. surveillance programmes.

It is interesting that in the Communication on the Functioning of Safe Harbour, the European Commission has described how different EU Member States data protection authorities handled data transfers to the U.S., remarking that only the German data protection authorities have expressed their concerns about transfers to the U.S., highlighting the high probability the Safe Harbour Adequacy Decision has been violated. In contrast with that view, the Irish and Luxembourg data protection authorities have confirmed that the transfers were aligned with their national data protection laws based on the Directive 95/46/EC. However, the cases before the Irish authority were referred to the Irish High Court, following a judicial redress, due to the inaction of the Irish Data Protection Commissioner in relation to U.S. surveillance programs[45].

Furthermore, the Communication on the Functioning of Safe Harbour, mentioned that Safe Harbour has been compromised as "all companies involved in the PRISM programme, and which grant access to U.S. authorities to data stored and processed in the U.S., appear to be Safe Harbour certified"[46]. It also added that these activities were performed contrary to the Safe Harbour Adequacy Decision which stated that any limitation to the Safe Harbor Principles must be limited only "to the extent necessary" to meet national security, public interest, or law enforcement requirements[47]. Additionally, the European Commission highlighted that, "in order for limitations and restrictions on the enjoyment of fundamental rights to be valid, they must be narrowly construed; they must be set forth in a publicly accessible law and they must be necessary and proportionate in a democratic society"[48].

[44] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM/2013/0847 final), available on https://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF.
[45] *Ibid*, p. 5.
[46] *Ibid*, p. 16.
[47] *Ibid.*
[48] *Ibid*.

Regarding individuals' data protection rights, in the Communication on the Functioning of the Safe Harbour, it is stated that "there are no opportunities for either EU or U.S. data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the U.S. surveillance programmes", and that "individuals and companies are thus not aware of what is being done with their data"[49].

However, besides all concerns explained in detail in both communications and in the Report from 2013, the European Commission's conclusion within the Communication on the Functioning of Safe Harbour, has not systematically addressed the main concerns – access and use of transferred personal data by the U.S. authorities, nor provides any roadmap for solving the identified issues. The European Commission's approach was limited to merely mention that "it is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate"[50].

This passive approach of the European Commission will be a repetitive, constant behaviour and overwhelmed by proactive non-governmental organisations that will initiate different procedures against the Safe Harbour Adequacy Decision (and its successor) resulting with the defeat of the European Commission's approach before the Court of Justice of the European Union.

5. The invalidation of the Safe Harbour Adequacy Decision

More than two years after the unveiling of the wide data collection practices of the U.S. authorities, the Court of Justice of the European Union, in October 2015, has decided to invalidate the Safe Harbour Adequacy Decision in a decision widely known as Schrems I judgment[51]. The invalidation decision of the Court of Justice of the European Union was in line with its case law related to data protection, especially the case law developed in the post Lisbon period, when the Charter and its data protection perspective, became legally binding[52].

[49] *Ibid,* p. 17.
[50] *Ibid*, p. 19.
[51] C-362/14, *Maximillian Schrems v Data Protection Commissioner*, judgment of 6 October 2015, ECLI:EU:C:2015:650.
[52] Terpan F., "EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?", European Papers, Volume 3, No 3, 2018, available on https://doi.org/10.15166/2499-8249/261, p. 1050.

a. The questions referred for a preliminary ruling

The case was initiated on 25 June 2013 Mr Max Schrems, an Austrian citizen, user of Facebook, lodged a complaint with the Irish Commissioner (data protection authority) by which he, in essence, asked the latter "to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data" as he considered the U.S. did not comply with the EU data transferring rules[53]. Based on the revelations made by Mr Edward Snowden concerning the activities of the U.S. intelligence services, Mr Schrems indicated that "the law and practice in force in the U.S. did not ensure adequate protection of the personal data held in its territory against the surveillance activities of its public authorities"[54].

As described in the description of the main proceedings made by the Court of Justice of the European Union in the Schrems I judgment, "[a]ny person residing in the EU who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the [U.S.]", being the personal data of these individuals then transferred from the EU to Facebook Inc. servers located in the U.S.[55]

As mentioned in the Communication on the Functioning of Safe Harbour, the Irish Commissioner's view was that it was not required to investigate the matters related to the Safe Harbour Adequacy Decision[56]. That Commissioner stated that the claim was "frivolous and vexatious" as the transfers of personal data from the EU to the U.S. were carried out within the framework of the Safe Harbour Adequacy Decision, and also remarked that any question related to the adequate level data protection in the U.S. had to be addressed in accordance with the adequacy decision in place[57].

Following the refusal of the Irish data protection authority to accept Mr Schrems's request, he challenged the data protection authority's decision before the High Court. As stated by the Court of Justice of the European Union, the Irish High Court remarked that, although the electronic surveillance of personal data transferred from the EU to the U.S. are objectives in the public interest, "the revelations made by Edward Snowden had demonstrated a 'significant

[53] Schrems I judgment, para 28.
[54] *Ibid*.
[55] *Ibid* 27.
[56] Communication on the Functioning of Safe Harbour, p. 5.
[57] Colonna L.: "Europe Versus Facebook: An Imbroglio of EU Data Protection Issues", Data Protection on the Move, Current Developments in ICT and Privacy, Data Protection, Law, Governance and Technology: Series Issues in Privacy and Data Protection, Springer, 2016, p. 32.

over-reach' on the part of the NSA and other federal agencies" [58]. In addition to that, the referring court especially mentioned the lack of effective redress (right to be heard) available to the EU citizens[59].

In a summarised explanation of the context, provided when submitting the request for a preliminary ruling, the High Court has remarked the Irish constitutional framework, mentioning that any interference with the right to privacy needs to be proportionate and in accordance with the law, and that any interception of electronic communications needs to be targeted and objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards, remarking that, if only Irish law was to be applied, "the Commissioner should have proceeded to investigate the matters raised by Mr Schrems"[60].

As stated in the paragraph 34 of the Schrems I judgment, the referring court has exposed its view that the Safe Harbour Adequacy Decision does not satisfy the requirements set out in Articles 7 and 8 of the Charter nor the principles described by the Court of Justice of the European Union in *Digital Rights Ireland and Others* judgment[61]. Then the Irish court in question has pointed out that "the right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards"[62].

As the Court of Justice of the European Union explains, "the High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings"[63]. The questions referred to the Court of Justice of the European Union were related to the power of a national data protection authority to investigate a complaint regarding

[58] Schrems I judgment, para 30.
[59] *Ibid*, para 31.
[60] *Ibid*, paras 32 and 33.
[61] *Ibid*, para 34.
[62] *Ibid*.
[63] *Ibid.* para 35.

transfers of personal data to a third country in a context where a European Commission's adequacy decision in the meaning of Directive's Article 25 applies[64]. However, the Court of Justice of the European Union decided to also address the validity of the Safe Harbour Adequacy Decision considering, among other reasons, that only it has the authority to invalidate a decision of the European Commission and that it is appropriate to provide a complete answer to the referring court[65].

Concerning the main doubt of the referring court regarding the power of the Member States, and more precisely EU Member States' data protection authorities, in relation to permitted actions when the European Commission adopts an adequacy decision to ensure free transfers of data to a third country, the Court of Justice of the European Union remarks that the Member States "cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection, emphasising that the measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality"[66].

Nevertheless, the validity of such adequacy decisions adopted by the European Commission, does not mean the exclusion of those decisions from any scrutiny by the national authorities nor the lack of individuals' right to start such scrutiny when they consider their data protection rights are violated. As specified in the Schrems I judgment, the Court of Justice of the European Union has aligned itself with the position of the Advocate General against the views of the European Commission. As expressed in the Opinion of the Advocate General Bot, the European Commission standpoint was that in the division of powers between the European Commission and the EU Member States has required that the national authorities are in charge of solving individual cases, while it was up to the European Commission the "general review of the application" of adequacy decisions[67]. Contrary to the European Commission's point of view, the Advocate General has stated that "the existence of a decision adopted by the Commission on the basis of Article 25(6) of Directive 95/46 cannot eliminate or even reduce the national

[64] *Ibid.* para 36.
[65] *Ibid*, para. 67.
[66] *Ibid*, para. 52.
[67] C-362/14, *Maximillian Schrems v Data Protection Commissioner*, Opinion of 23 September 2015, ECLI:EU:C:2015:627, paras. 58 to 60.

supervisory authorities' powers under Article 28 of that directive", having the national data protection authorities the power to form "their own opinion on the general level of protection ensured by a third country and from drawing the appropriate conclusion when they determine individual cases"[68]. This view of the Advocate General was further endorsed in the Schrems I judgment, where the Court of Justice of the European Union stated that an adequacy decision adopted by the European Commission "cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive"[69]. In that line, based on the reasoning that there are no legislative limitations regarding personal data transfers to third countries, the Court ruled that nothing prevents a data protection authority "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"[70].

From the given context, it can be concluded that the European Commission was interested in excluding national data protection authorities from any involvement in assessing adequacy decisions for transferring personal data to third countries, limiting their role to simply verifying whether such decisions are in place or not. However, the Court of Justice of the European Union has recognised the important role of data protection authorities, affirming their right to investigate allegations about violations of data protection rights connected to data transferred based on adequacy decisions and, in case they consider such allegations are founded, to engage with national courts, based on their national legislation, "in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity"[71].

b. Court's assessment of the Safe Harbour Adequacy Decision

From the perspective of data transfers to the U.S., it is much more relevant the Court of Justice of the European Union assessment regarding the respect in the U.S. for privacy and fundamental rights in general.

When it comes to the scrutiny of the adequacy decision, it is interesting the analysis of the Advocate General regarding the notion of "adequacy". He stated in the paragraphs 141 and 142

[68] *Ibid,* para 61.
[69] Schrems I judgment, para 53.
[70] *Ibid*, point 1 of the operative part.
[71] *Ibid*, para 65.

of his Opinion, that a country is providing an adequate level of protection "only where, following a global assessment of the law and practice in the third country in question, it is able to establish that that third country offers a level of protection that is essentially equivalent to that afforded by the directive, even though the manner in which that protection is implemented may differ from that generally encountered within the European Union[72]. Although the English word 'adequate' may be understood, from a linguistic viewpoint, as designating a level of protection that is just satisfactory or sufficient, and thus as having a different semantic scope from the French word 'adéquat' ('appropriate'), the only criterion that must guide the interpretation of that word is the objective of attaining a high level of protection of fundamental rights, as required by Directive 95/46"[73]. In the next paragraph of the opinion, the Advocate General concludes that the assessment whether a country has adequate level of data protection "must focus on two fundamental elements, namely the content of the applicable rules and the means of ensuring compliance with those rules"[74].

The Court of Justice of the European Union's position is consonant with the one of the Advocate General, as it has stated that a "third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order", but that "adequate level of protection" means that a third country provides 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", remarking that such requirement is necessary to ensure the EU data protection standards are not circumvented when transferring personal data to third countries[75].

Similarly to the expressed by the Advocate General, the Court of Justice of the European Union in its judgment stated that the "Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country"[76]. Therefore, the mere existence of rules eventually aligned with the EU data

[72] C-362/14, *Maximillian Schrems v Data Protection Commissioner*, Opinion of 23 September 2015, ECLI:EU:C:2015:627, paras. 141 and 142.
[73] C-362/14, *Maximillian Schrems v Data Protection Commissioner*, Opinion of 23 September 2015, ECLI:EU:C:2015:627, para. 141.
[74] *Ibid*, para. 142.
[75] Schrems I judgment, para. 73.
[76] *Ibid*, para. 75.

protection standards, is not sufficient as long as there are not accompanied by their implementation in practice. Regarding that requirement, the Court is clear when affirms that the trust on a system that protects personal data depends "essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice"[77].

Besides, the analysis of the "adequacy" of third country's legal framework should not be one-off exercise but should be regular, in order to continuously validate that third country's data protection standards are aligned with the EU's ones during the entire validity of the adequacy decision. The Court of Justice of the European Union has pointed out that "it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard"[78].

Regarding the scope of application of the Safe Harbour Adequacy Decision, the Court of Justice of the European Union identified that the Safe Harbor Principles are applicable only to self-certified organisations (companies importing personal data from the EU), but that "United States public authorities are not required to comply with them"[79]. The Court of Justice emphasises that the Safe Harbour Adequacy Decision does not contain "sufficient findings regarding the measures by which the United States ensures an adequate level of protection"[80]. In the next paragraph the Court paid attention to Safe Harbour Adequacy Decision's Annex I, paragraph 4, which mentioned that there can be implemented limitations regarding the applicability of the Safe Harbour Principles when its necessary to comply with different national security, public interest, or law enforcement requirements, as well as with obligations emerging from statutes, government regulations, or case law. These collision between data protection and other legal values that need to be protected show, as already mentioned in this work, that there is an imbalance affecting data protection rights when they are in conflict with other legal provisions in the U.S. This imbalance was identified by the Court of Justice of the European Union when it remarked that the text of the Safe Harbour's Adequacy Decision's

[77] *Ibid*, para. 81.
[78] *Ibid*, para 76.
[79] *Ibid*, para. 82.
[80] *Ibid,* para 83.

Annex IV, Part B, imposed the obligation to U.S. entity to leave Safe Harbor Principles aside in case of conflict with an U.S. law provision, which in practice weakens the data protection standards that any adequacy decision should ensure[81]. Therefore, if the Safe Harbor Principles are in collision with any legislative act in the U.S., such principles would be annihilated along with the personal data protection chain, breaking the essentially equivalent level of protection that should permanently apply to the personal originated in the EU.

Following the obligation to permanently monitor whether a third country legal framework and practices meet EU standards, the Court of Justice of the European Union remarks the assessment made by the European Commission and published in the Communication on Rebuilding Trust and the Communication on the Functioning of Safe Harbour, which confirmed the ability of U.S. authorities to access personal data transferred to the U.S. "in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security"[82].

In connection with the aforementioned, the Court of Justice of the European Union noted the deficiencies of the supervisory and dispute resolution mechanisms established by the Safe Harbour Adequacy Decision in paragraph 90 of the Schrems I judgment. Echoing the views of the Advocate General, expressed in paragraph 212 of his Opinion, the Court confirmed what is clearly evident from the Safe Harbour Adequacy Decision: the absence of any redress mechanism for activities carried out by U.S. public authorities when processing personal data transferred from the EU.

The inability of individuals to access any effective redress mechanism concerning the processing of their personal data significantly impacts the assessment of the legality of the adequacy decision in question. This is particularly important to consider in light of the extensive case law of the Court of Justice of the European Union, which has consistently reaffirmed that any restrictions on the protection of personal data can only be applied if they are strictly necessary. This principle was also confirmed in paragraph 92 of the Schrems I judgment, which cites the judgment in the case of *Digital Rights Ireland and Others*. This position is backed by the views of the Court expressed for example in the judgment Satakunnan Markkinapörssi and Satamedia, where it stated that when balancing between the right to freedom of expression and the right to privacy, "the protection of the fundamental right to privacy requires that the

[81] *Ibid*, para. 85 and 86.
[82] *Ibid*, para 90.

derogations and limitations in relation to the protection of data provided for in the chapters of the directive referred to above must apply only in so far as is strictly necessary"[83].

Afterwards, the Court proceeded to assess whether the legal framework was limited to what is "strictly necessary" and provided its ultimate conclusion, which served as basis for invalidating the Safe Harbour Adequacy Decision. In its analysis the Court found 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"[84]. The Court of Justice of the European Union especially indicated two very specific and major deficiencies of the U.S. legal framework which were considered to undermine the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter and the right to effective judicial protection as established in Article 47 of the Charter. The right expressed in Article 7 of the Charter was undermined by the power of the public authorities to have lawful access on a generalised basis to the content of electronic communications[85]. At the same time, the right recognised in Article 47 of the Charter, which is qualified in this judgment as "inherent in the existence of the rule of law", was overlooked for individuals whose data were transferred to the U.S., due to the absence of any mechanism available to them to pursue legal remedies in order to access personal data relating to them or to obtain the rectification or erasure of such data[86]. Regarding the restrictions imposed on EU Member States' data protection authorities' investigatory powers, the Court of Justice of the European Union found that such restrictions were contrary to Article 28 of Directive 95/46, read in light of Article 8 of the Charter. The Court reaffirmed the significance of these authorities in the EU's data protection framework, confirming that the scope of their powers is defined by Article 8 of the Charter and Directive 95/46/EC and cannot be redefined by an adequacy decision[87].

[83] C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, judgment of 16 December 2008, ECLI:EU:C:2008:727, para. 56.
[84] Schrems I judgment, para. 93
[85] *Ibid,* para. 94.
[86] *Ibid,* para. 95.
[87] *Ibid*, para. 99.

The mentioned crucial deficiencies identified by the Court of Justice of the European Union have led to the invalidation of the Safe Harbour Adequacy Decision[88].

The Safe Harbour Adequacy Decision was invalidated on 6 October 2015, although the European Commission had relevant information in 2013 that could have prevented further transfers of personal data under that defective framework. That year, the European Commission had access to the Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection, as well as the Communication on Rebuilding Trust and the Communication on the Functioning of Safe Harbour, which severely criticised the operation of the Safe Harbour Principles and highlighted the significant deficiencies affecting individuals' data protection rights. However, the European Commission did not take any effective immediate action to bring data transfers to the U.S. into compliance. On the contrary, as the European Commission was likely anticipating a decision from the Court of Justice of the European Union (at least from the moment the Advocate General provided his conclusions), it left the invalidation to the Court rather than restricting or suspending the Safe Harbour Adequacy Decision while it was in the midst of negotiations with the U.S. on a new data transfer framework called Privacy Shield[89]. That new data transferring framework, entered into force less than one year after the invalidation of the Safe Harbour Adequacy Decision and implemented many of the defective approaches from the previously invalidated framework.

6. Reloaded data transfers with repeated deficiencies: Privacy Shield Adequacy Decision

On November 6, 2015, exactly a month after the judgment in the case Schrems I and the invalidation of the Safe Harbour Adequacy Decision, the European Commission communicated that it "will continue and finalise negotiations for a renewed and sound framework for transatlantic transfers of personal data, which must meet the requirements identified in the Court ruling, notably as regards limitations and safeguards on access to personal data by U.S. public authorities"[90].

[88] *Ibid*, paras. 105 and 106.
[89] ANNEX 1 (Letter of Penny Pritzker to Věra Jourová, from July 7, 2016) of the Privacy Shield Adequacy Decision.
[90] Press Release of November 6, 2015, European Commission, available on https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_15_6015/IP_15_6015_EN.pdf.

The result of the negotiations, that started in 2014 between the EU and the U.S. to improve the U.S. protection of transferred personal data, was the adoption of the Privacy Shield Adequacy Decision on 12 July 2016. This new adequacy decision had the objective to solve the deficiencies found by the Court of Justice of the European Union in Schrems I judgment. In that sense, the European Commission in the Privacy Shield Adequacy Decision stated that the "Court of Justice criticised the lack of sufficient findings in Decision 2000/520/EC regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and the existence of effective legal protection against interference of that kind"[91].

The Privacy Shield framework has been criticised for following the approach of the Safe Harbour framework, as it is based on a series of informal letters addressed by U.S. authorities to the EU that do contain binding legal guarantees. In that sense, the Privacy Shield framework was not designed as an external agreement based on Article 218 of the Treaty on the Functioning of the European Union[92], and as did not contain mutually binding commitments, and is considered as a soft law by some authors[93].

In line with the Safe Harbour Adequacy Decision, the Privacy Shield Adequacy Decision relied on a set of principles known as the EU-U.S. Privacy Shield Framework Principles (hereinafter: Privacy Shield Principles), which needed to be implemented by U.S. organisations that, by a system of self-certification, would commit to accommodate their data protection practices to such principles, and which enabled them to receive personal data from the EU without any additional condition. The principles such companies would need to comply with were comparable to the Safe Harbor Principles. These new (old) principles brought along with the Privacy Shield framework were: Notice, Data Integrity and Purpose Limitation, Choice, Security, Access, Recourse, Enforcement and Liability, and Accountability for Onward

[91] Privacy Shield Adequacy Decision, recital 11.
[92] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (OJ 2016 C 202, p. 1).
[93] Fahey E. & Terpan F., "The Future of the EU-US Privacy Shield", The Routledge Research Handbook of Transatlantic Relations, 2023, Abingdon, United Kingdom, available on https://doi.org/10.4324/9781003283911, p. 223.

Transfers[94]. However, the new framework brought some enhancement in the fields of transparency, onward transfers, recourse mechanisms, enforcement and liability[95].

However, besides all aspects related to the processing of transferred personal data carried out by the U.S. companies that were receiving data from the EU, the main concern to be addressed by the new data transferring framework was related to the legal framework applicable to the interferences with the fundamental rights to respect for private life and to protect personal data when the public authorities carry out national security or law enforcement activities. The general position of the European Commission was aligned with the introductory statement that any deviation from the Privacy Shield Principles "is limited to the extent necessary to meet national security, public interest or law enforcement requirements"[96]. This consideration by the European Commission regarding the limitation of privacy and fundamental rights will be shown to have only declaratory strength and lack substance, with the Privacy Shield Adequacy Decision ultimately having the same deficiencies as the Safe Harbour Adequacy Decision.

a. Processing of data for national security purposes

Regarding the access and use of transferred personal data by U.S. public authorities for national security purposes, the European Commission in the new adequacy decision remarked the improvements brought by the U.S. Presidential Policy Directive 28 (hereinafter: PPD-28) issued on January 2014[97]. However, it is interesting to note that the PPD-28 was already existing at the moment the procedure for a preliminary ruling in the Schrems I case was initiated (July 2015), but anyway it did not have any impact on the assessment how the U.S. authorities process transferred personal data.

Anyway, the European Commission decided to base on the PPD-28 a significant part of its explanations regarding the improvements the Privacy Shield Adequacy Decision brought in comparison to the invalidated adequacy decision. The European Commission pointed out the positive impact of the PPD-28 on all individuals whose data have been processed by the U.S. authorities for national security purposes, and enumerated the following requirements brought by the PPD-28:

---

[94] Title II of Annex II to the Privacy Shield Adequacy Decision.
[95] Vrbljanac, D., "Managing Innovative Company's Capital: The Case of Personal Data Transfer", Zb. Prav. fak. Sveuč. u Rij., Vol. 39, No. 4, 2018, available on https://hrcak.srce.hr/file/318741, p. 1785.
[96] *Ibid*, recital 64.
[97] Presidential Policy Directive -- Signals Intelligence Activities, Policy Directive/PPD-28 of January 17, 2014, available on: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities#_ftn5

"(a) the collection of signals intelligence must be based on statute or Presidential authorisation, and must be undertaken in accordance with the U.S. Constitution (in particular the Fourth Amendment) and U.S. law;

(b) all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside;

(c) all persons have legitimate privacy interests in the handling of their personal information;

(d) privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities;

(e) U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of their nationality or where they might reside"[98].

In the Privacy Shield Adequacy Decision's recitals explaining the PPD-28, the European Commission stated that the "PPD-28 directs that signals intelligence may be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purpose (e.g. to afford a competitive advantage to U.S. companies) and specifies that decisions about intelligence collection are not left to the discretion of individual intelligence agents, but are subject to the policies and procedures", as well it is clarified that "intelligence collection shall always be 'as tailored as feasible'", and that there is a "general rule of prioritisation of targeted over bulk collection"[99]. The framework defined by the PPD-28 was sufficient to gain the trust of the European Commission, which concluded that it was credible the assurance provided by the Office of the Director of National Intelligence of the U.S. affirming that "bulk collection is neither 'mass' nor 'indiscriminate', and that the exception does not swallow the rule"[100].

In that regard, it is interesting the easy approach of the European Commission lacking additional scrutiny regarding the statement provided by the Office of the Director of National Intelligence which is contradictory at first sight since "bulk" and "mass" or "indiscriminate" could be used

[98] Privacy Shield Adequacy Decision, recital 69.
[99] *Ibid*, recital 70 and 71.
[100] *Ibid*, recital 71.

as equal terms. The explanation given in the Privacy Shield Adequacy Decision can be found in the Robert S. Litt's letter that reads as follows:

> "As an example, the Intelligence Community may be asked to acquire signals intelligence about the activities of a terrorist group operating in a region of a Middle Eastern country, that is believed to be plotting attacks against Western European countries, but may not know the names, phone numbers, e-mail addresses or other specific identifiers of individuals associated with this terrorist group. We might choose to target that group by collecting communications to and from that region for further review and analysis to identify those communications that relate to the group. In so doing, the Intelligence Community would seek to narrow the collection as much as possible. This would be considered collection in 'bulk' because the use of discriminants is not feasible, but it is neither 'mass' nor 'indiscriminate'; rather it is focused as precisely as possible.
>
> (…)
>
> Thus, the Intelligence Community's 'bulk' collection is not 'mass' or 'indiscriminate,' but involves the application of methods and tools to filter collection in order to focus the collection on material that will be responsive to policy-makers' articulated foreign intelligence requirements while minimizing the collection of non-pertinent information, and provides strict rules to protect the non-pertinent information that may be acquired"[101].

In addition, besides trying to explain the difference between "mass", "indiscriminate" and "bulk" collection, in the Privacy Shield Adequacy Decision the European Commission has pointed out that, based on PPD-28, the Intelligence Community must prioritise alternatives that would allow the conduct of targeted signals intelligence and concludes that "bulk collection will only occur where targeted collection via the use of discriminants — i.e. an identifier associated with a specific target (such as the target's e-mail address or phone number) — is not possible 'due to technical or operational considerations'"[102].

The European Commission also stated, based on the inputs received from the Office of the Director of National Intelligence, that in a situation where specific identifiers cannot be used for data collection, the Intelligence Community "will seek to narrow the collection 'as much as

[101] *Ibid,* Annex VI.
[102] *Ibid*, recital 72.

possible'", which would target bulk collection in two ways: on one hand it would relate to "specific foreign intelligence objectives" and on the other hand the collection technics would be designed to collect the less quantity of irrelevant data as possible[103].

Finally, the European Commission in the Privacy Shield Adequacy Decision has remarked that the collected intelligence signals would be used only for six national security purposes: detect and counter threats stemming from espionage, terrorism, weapons of mass destruction, threats to cybersecurity, to the Armed Forces or military personnel, as well as transnational criminal threats related to the other five purposes[104].

It is impossible to avoid tracing connecting lines between the mentioned activities carried out by the U.S. authorities and the invalidated EU's Data Retention Directive, which was aiming at harmonising "Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks […], in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law"[105]. In connection with the mentioned, regarding the possibility of collecting everyone's data within certain territory, it is interesting that it seems that the European Commission decided to ignore the already mentioned *Digital Rights Ireland and Others* judgment, where the Court of Justice of the European Union disapproved the approach implemented in the Data Retention Directive, stating that it "affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy"[106].

In the recital 78 of the Privacy Shield Adequacy Decision it has been stated that the collection of personal data transferred to U.S. self-certified organisations under the Privacy Shield

[103] *Ibid*, recital 73.
[104] *Ibid*, recital 74.
[105] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).
[106] C-293/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, judgment of 8 April 2014, ECLI:EU:C:2014:238, para. 58.

framework, can be accessed by the U.S. intelligence authorities in accordance with the Foreign Intelligence Surveillance Act (hereinafter: FISA) or based on the so-called National Security Letters (hereinafter: NSL) applicable to the Federal Bureau of Investigation (hereinafter: FBI).

Regarding FISA, the Privacy Shield Adequacy Decision clarified that, based on its section 702, two programs have been conducted: PRISM and UPSTREAM, within which searches have been targeted "through the use of individual selectors that identify specific communications facilities", and provided the conclusion that, based on "the Privacy and Civil Liberties Oversight Board (PCLOB), Section 702 surveillance 'consists entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made'"[107]. In order to minimise the impact, the Privacy and Civil Liberties Oversight Board remarked that U.S. authorities provided "empirical evidence which shows that access requests through NSL and under FISA, both individually and together, only concern a relatively small number of targets when compared to the overall flow of data on the internet"[108].

Considering the previously mentioned Report from 2013, and the European Parliament's Report on NSA surveillance from 2014[109], it is interesting that the European Commission in 2016 decided to support the "empirical evidence" provided by the U.S. authorities and include it as an argument for providing the status of adequacy to the Privacy Shield framework. It is important to analyse the figures behind the statement on "relatively small number of targets when compared to the overall flow of data on the internet". The Report from 2013 states that "the U.S. confirmed that 1.6% of all global internet traffic is 'acquired' and 0.025% of it is selected for review; hence 0.0004% of all global internet traffic is looked at by NSA analysts, and also mentions that the vast majority of global internet traffic consists of high-volume streaming and downloads such as television series, films and sports, as well as that communications data makes up a very small part of global internet traffic"[110]. In line with that, the European Parliament in its Report on NSA surveillance from 2014, "points specifically to U.S. NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading U.S. internet companies (PRISM programme), the

[107] *Ibid*, recital 81. The Privacy and Civil Liberties Oversight Board was established in section 801 of the Implementing Recommendations of the 9/11 Commission Act of 2007, available on https://www.congress.gov/110/plaws/publ53/PLAW-110publ53.pdf.
[108] Privacy Shield Adequacy Decision, recital 82.
[109] Report on the U.S. NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (Report - A7-0139/2014), available on https://www.europarl.europa.eu/doceo/document/A-7-2014-0139_EN.html.
[110] Report from 2013, section 3.1.2., p. 11.

analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN), access to computer and telephone networks, and access to location data, as well as to systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), the decryption programme (Edgehill), the targeted 'man-in-the-middle attacks' on information systems (Quantumtheory and Foxacid programmes) and the collection and retention of 200 million text messages per day (Dishfire programme)"[111]. It is clear that the "empirical evidence" used as argument by the European Commission is not relevant for assessing the notion of bulk collection of data, and that the scope of individuals affected by the activities of the U.S. intelligence community is much higher when the raw numbers are properly analysed and internet streaming and downloads excluded from the equation.

Anyway, besides the judgment of the Court of Justice of the European Union in *Digital Rights Ireland and Others* case, the Report from 2013 and the European Parliament's Report on NSA surveillance, the European Commission concluded that "there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the United States under the EU-U.S. Privacy Shield to what is strictly necessary to achieve the legitimate objective in question, that it conforms with the standard set out by the Court of Justice in the Schrems judgment affirming that neither will there be unlimited collection and storage of data of all persons, and that surveillance activities touch only a fraction of the communications traversing the internet"[112].

b. Legal protection against U.S. intelligence community activities

One of the reasons why the Court of Justice of the European Union invalidated the Safe Harbour Adequacy Decision, was related to lack of available legal protections against personal data processing activities caried out by the U.S. intelligence authorities.

Concerning that background, the European Commission clearly stated that "intelligence activities by U.S. authorities are subject to extensive oversight from within the executive branch[113]. The Privacy Shield Adequacy Decision emphasised that, following PPD-28, the U.S. intelligence community was required to implement measures to enable oversight of mechanisms aimed at protecting personal data. It further specified the oversight layers, which

[111] European Parliament's Report on NSA surveillance, title "Main Findings", point 2.
[112] Privacy Shield Adequacy Decision, recital 88 and 90.
[113] *Ibid*, recital 93.

included civil liberties or privacy officers, Inspectors General, the Civil Liberties Protection Officer of the Office of the Director of National Intelligence, the Privacy and Civil Liberties Oversight Board, and the President's Intelligence Oversight Board. Additionally, the European Commission assessed that the roles of specific working bodies (committees) within the U.S. Congress included the protection of, among other things, personal data transferred from the EU. That conclusion emerges from the recital 102 of the Privacy Shield Adequacy Decision where it is stated that "the House and Senate Intelligence and Judiciary Committees, have oversight responsibilities regarding all U.S. foreign intelligence activities, including U.S. signals intelligence". However, the role, independence, powers, expertise and structure of such Congressional committees have essential differences comparing with the independent authorities to which Article 8(3) of the Charter refers and which were further defined in Article 28 of the Directive 95/46/EC and currently are described in Chapter VI of the General Data Protection Regulation, that there are no points of connection between them.

Also, as oversight mechanism the Privacy Shield Adequacy Decision has pointed out the role of the Foreign Intelligence Surveillance Court (hereinafter: FISC), an entity that already existed in times of the Safe Harbour Adequacy Decision (although its role was not mentioned there), the Foreign Intelligence Surveillance Court of Review and, ultimately, the Supreme Court of the U.S. However, as explicitly stated in the Privacy Shield Adequacy Decision, "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"[114]. More precisely, the FISC is not a regular type of tribunal, operates *ex parte*, that is without representation or notification to the accused, due to U.S. national security reasons, and therefore individuals from the EU whose personal data are transferred cannot exercise their data protection rights before it[115].

Besides the oversight mechanisms, in the Schrems I judgment and related Advocate General's opinion, special attention was given to the redress processes. The Advocate General in the paragraph 212 of his opinion stated that "the Commission has itself pointed out that there are no opportunities for citizens of the Union to obtain access to or rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their

[114] *Ibid,* recital 109.

[115] Rodriguez S., „The United States of Surveillance: A Review of America's Mass Surveillance Laws, Programs, and Oversight", DHSI Conference & Colloquium, Volume 3, Iss. 2, 2021, https://doi.org/10.21428/f1f23564.f20c77b2.

personal data taking place under the United States surveillance programmes". In line with that position, Schrems I judgment in its paragraph 90, in essence communicates the same idea.

Therefore, the context related to the Schrems I judgment required from the European Commission to implement significant improvements with regard to redress mechanisms available to EU individuals whose personal data are affected by transfers to the US. In relation with that concern, the Privacy Shield Adequacy Decision in first place mentioned the "possibility for individuals to bring a civil cause of action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed; to sue U.S. government officials in their personal capacity ('under colour of law') for money damages; and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the United States"[116]. In second place the Privacy Shield Adequacy Decision also mentioned other mechanisms available to EU data subjects based on specific laws[117].

However, it was also clarified that "the available causes of action are limited and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show 'standing', which restricts access to ordinary courts"[118]. Therefore, showing "standing" would turn almost impossible as surveillance measures are classified, which limits the availability of proves individuals need to present in order to initiate the relevant process. Besides that, the mentioned recital also remarks that some activities carried out on specific legal basis (such as the E.O. 12333)[119], were by default excluded from any redress mechanism available to EU data subjects. Therefore, it can be concluded that the mentioned redress mechanisms are much more restrictive in the U.S. than in the EU, and that in some cases are not available at all.

Considering the restrictions related to the access to effective redress mechanism and the criticism expressed in that regard, in the negotiations the U.S. authorities accepted to include a new avenue for addressing redress requests of individuals whose data are transferred from the

[116] Privacy Shield Adequacy Decision, recital 112.
[117] *Ibid,* recital 113.
[118] *Ibid,* recital 115.
[119] The U.S. Constitution does not refer to the term "executive order". However, the commonly used description of executive orders was provided in a report issued in 1957 by the House Government Operations Committee Executive, in which it was defined that executive orders are directives or actions by the U.S. President, and may have the force and effect of law in case they are derived from the Constitution or statute. Chu, V.S., Garvey, T.: "Executive Orders: Issuance, Modification, and Revocation", Congressional Research Service, 2014, available on https://sgp.fas.org/crs/misc/RS20846.pdf, p. 1.

EU to the US. This new redress avenue was called Privacy Shield Ombudsperson and was established by the U.S. Secretary of Sates, John F. Kerry, which was, in his own words, consistent with the PPD-28[120], designed to be independent from the intelligence community, and to be objectively and free from any improper influence liable to have an effect on the response to be provided[121].

In the Privacy Shield Adequacy Decision, the European Commission transposed the words of U.S. authorities, stating that the objective of establishing this new mechanism was to ensure that individual complaints were properly investigated and addressed, and that individuals received independent confirmation that U.S. laws had been complied with, or, in cases of violation, that non-compliance had been remedied. It also indicated that the Privacy Shield Ombudsperson was provided with adequate investigatory powers related to the operations carried out by the U.S. intelligence community[122]. In line with the position of the U.S. authorities, the European Commission celebrated the implementation of the Privacy Shield Ombudsperson as a body that would guarantee independent oversight and individual redress along with effective remediation powers[123].

The European Commission compared the Privacy Shield framework against the Schrems I judgment, and in this context, cited the position of the Court of Justice of the European Union on the necessity for third-country legislation to provide effective redress, concluding that it "has confirmed that such legal remedies are provided for in the United States, including through the introduction of the Ombudsperson mechanism"[124]. However, the Privacy Shield Ombudsperson had many deficiencies, from its independence, which will be addressed by the Court of Justice of the European Union, to the issue of not providing complainants substantial information on the results of its investigations. In that sense, the Privacy Shield Ombudsperson would "neither confirm nor deny whether the individual has been the target of surveillance nor [would] confirm the specific remedy that was applied", limiting its answer just to confirm "(i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-

[120] Privacy Shield Adequacy Decision, Annex III.
[121] *Ibid*, recital 121.
[122] *Ibid*, recital 117.
[123] *Ibid*, recitals 117 and 118.
[124] *Ibid*, recital 124.

compliance has been remedied"[125]. After the invalidation of the Privacy Shield Adequacy Decision, the same approach, which substantially limits the content of the response provided to complainants, was implemented in the EU-U.S. Data Privacy Framework Adequacy Decision[126].

c. Adequate level of protection under the EU-U.S. Privacy Shield

After starting the negotiating process with the U.S. in 2014, the European Commission proceeded to issue an adequacy decision for the Privacy Shield framework, which was enacted after being accepted by the majority of Member States as stipulated in the Article 31 of the Directive.

The Privacy Shield Adequacy Decision was subject to periodic reviews, to assess "whether the findings relating to the adequacy of the level of protection ensured by the United States under the EU-U.S. Privacy Shield are still factually and legally justified"[127]. In line with that, and as was already established by the previously invalidated adequacy decision, the Privacy Shield Adequacy Decision included a mechanism to repeal or suspend the decision if "the level of protection offered by the Privacy Shield can no longer be regarded as essentially equivalent to the one in the Union, or where there are clear indications that effective compliance with the Principles in the United States might no longer be ensured, or that the actions of U.S. public authorities responsible for national security or the prevention, investigation, detection or prosecution of criminal offenses do not ensure the required level of protection"[128]. Needless to say, the Court of Justice of the European Union declared invalid the Privacy Shield Adequacy Decision without the suspension process been ever activated by the European Commission.

It is important to remark that the conditions for triggering the suspension process were the following:

> "(a) indications that the U.S. authorities do not comply with the representations and commitments contained in the documents annexed to this decision, including as regards the conditions and limitations for access by U.S. public authorities for law enforcement,

[125] *Ibid*, ANNEX III, Annex A section 4.e.
[126] 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-U.S. Data Privacy Framework (OJ 2023 L 231, p. 118).
[127] Privacy Shield Adequacy Decision, recital 145.
[128] *Ibid*, recital 150.

national security and other public interest purposes to personal data transferred under the Privacy Shield;

(b)failure to effectively address complaints by EU data subjects; in this respect, the Commission will take into account all circumstances having an impact on the possibility for EU data subjects to have their rights enforced, including, in particular, the voluntary commitment by self-certified U.S. companies to cooperate with the DPAs and follow their advice; or

(c) failure by the Privacy Shield Ombudsperson to provide timely and appropriate responses to requests from EU data subjects"[129].

The listed conditions for activating the suspension process were related to infringements of the Privacy Shield framework. However, it may not be possible to claim that the framework's rules were ever broken, while, in reality, the permissiveness of the data transfer rules adopted under the Privacy Shield Adequacy Decision (particularly regarding the activities of the U.S. intelligence community and the lack of effective redress mechanisms) was, in fact, the reason for the invalidation of that adequacy decision.

Since the adoption of the Privacy Shield Adequacy Decision and until its invalidation, the Privacy Shield framework was subject to three annual reviews. In the European Commission's reports from 2017 and 2018, it was explicitly stated that the U.S. "*continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield"* [130] [131]. The European Commission's report from 2019 did not contain such explicit wording, but anyway positively assessed that it "noted a number of improvements in the functioning of the framework as well as appointments to key oversight bodies and remarked the necessity to implement a set of measures to better ensure the effective functioning of the Privacy Shield in practice" [132].

In any case, it seems that the European Commission intentionally avoided, or at least failed to properly assess, the Privacy Shield framework prior to adopting an adequacy decision based on that framework. It could also be argued that the European Commission did not strictly follow the concepts outlined by the Court of Justice of the European Union, particularly in the Schrems

[129] *Ibid*, recital 151.
[130] Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, Brussels, 18.10.2017, COM(2017) 611 final.
[131] Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield, Brussels, 19.12.2018, COM(2018) 860 final.
[132] Report from the Commission to the European Parliament and the Council, on the third annual review of the functioning of the EU-U.S. Privacy Shield, Brussels, 23.10.2019, COM(2019) 495 final.

I and *Digital Rights Ireland and Others* judgments, sealing the fate of the Privacy Shield Adequacy Decision from the moment it was adopted.

From this perspective, it can be confirmed once again that the transatlantic commercial relationship is a two-way street, just like any other relationship of that kind, and that the interest of U.S. companies in providing services in the EU reflects the interest of EU companies in maintaining smooth business connections with their U.S. counterparts, while massive transfers of personal data increasingly occur in the background of such business activities. In that context, one conclusion could be that the interest of the European Commission is actually to find relatively fast and easy-to-implement approaches rather than long-lasting, fundamental rights-compliant solutions for EU-U.S. data transfers.

7. An expected outcome: The invalidation of the Privacy Shield Adequacy Decision

After delivering the judgment in the Schrems I case, the problematic related to personal data transfers to the U.S. continued, and led to a second case initiated by Mr Schrems, which ended with the invalidation of the Privacy Shield Adequacy Decision in the so-called Schrems II judgment[133].

As outcome of the Schrems I judgment, the Irish High Court annulled the Commissioner's rejection of Mr Schrems's complaint related to the transfers of personal data to the U.S.; consequently, the Commissioner had to reopen the case and assess the basis for the data transfers. During the investigation carried out by the Irish Commissioner, Facebook Ireland indicated that it has been using standard contractual clauses as data transferring mechanism[134]. Considering the changed context, the Commissioner asked Mr Schrems to reformulate his complaint[135]. After that, Mr Schrems asked the Irish Commissioner to stop data transfers to the U.S., following which the Commissioner questioned the validity of the adequacy decision and

[133] C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, judgment of 16 July 2020, ECLI:EU:C:2020:559.
[134] Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).
[135] Schrems II judgment, para. 54.

forwarded the request to the Irish High Court, which then referred the matter to the Court of Justice of the European Union[136].

It is interesting to mention the role of the U.S. authorities in the process before the High Court that led to the submission of the request for a preliminary ruling by the Court of Justice of the European Union. We have already seen that, in order to establish and maintain data transfers from the EU to the U.S., the U.S. authorities initially introduced self-certification in the very first framework for data transfers and later created the role of the Privacy Shield Ombudsperson. However, after the Schrems I judgment, the U.S. authorities engaged directly with the High Court. The active approach of the U.S. authorities expanded to the judiciary arena, granting to the U.S. the status of *amicus curiae* which was justified by the High Court as follows:

> "The United States has a significant and bona fide interest in the outcome of these proceedings. At issue in the proceedings is the assessment, as a matter of EU law, of the applicant's law governing the treatment of EU citizens' data transfer to the US. The imposition of restrictions on the transfer of such data would have potentially considerable adverse effects on EU-U.S. commerce and could affect U.S. companies significantly" [137].

However, as we will see, the involvement of the U.S. did not affect the already determined fate of the Privacy Shield Adequacy Decision.

The referring court provided an analysis of the legal framework and activities carried out by the U.S. authorities along with its request for a preliminary ruling. This analysis noted that, based on Section 702 of the FISA, the Attorney General and the Director of National Intelligence could, with FISC approval, conduct surveillance activities on individuals who were not U.S. citizens located outside the country to obtain 'foreign intelligence information', the High Court specified that, under the PRISM program, Internet service providers have been required to supply the NSA with all communications to and from a 'selector,' while, under the UPSTREAM program, telecommunication companies had to "allow the NSA to copy and filter Internet traffic flows in order to acquire communications from, to, or about a non-U.S. national associated with a 'selector'"[138]. The referring court also indicated that, to circumvent the

[136] Tylor M.: "*Transatlantic Jurisdictional Conflicts in Data Protection Law*", Cambridge University Press, 2023, p. 202.
[137] *Ibid*, p. 202.
[138] Schrems II judgment, paras. 61 and 62.

implementation of FISA restrictions, the NSA has accessed underwater telecommunication cables before entering the U.S., in accordance with E.O. 12333[139]. The High Court expressed its concerns regarding the activities of the U.S. intelligence community, pointing out that the massive collection of personal data violates the level of protection provided by Articles 7 and 8 of the Charter, and noted that the redress mechanisms available to EU citizens were insufficient and not comparable to those available to U.S. citizens, adding that the data collection activities based on E.O. 12333 fell outside the scope of any redress mechanism[140]. Finally, the referring court expressed its well-founded concerns regarding the role of the Privacy Shield Ombudsperson concluding that its authority cannot be compared to the one of a tribunal in the meaning of Article 47 of the Charter[141].

The referring court submitted a set of questions related to the applicability of standard contractual clauses, however, in this work we will focus our attention on the assessment the Court of Justice of the European Union provided in relation to the Privacy Shield Adequacy Decision. The main question to address here was related to Mr Schrems' consideration that the U.S. has not ensured an adequate level of protection, which led to a process before the Irish data protection authority and subsequently before the referring court. As the referring court was "unsure whether Mr Schrems's doubts as to the adequacy of the level of protection ensured in that third country are well founded, despite the subsequent findings of the Commission in the Privacy Shield Decision"[142], the Court of Justice of the European Union, sharing the views of the Advocate General, concluded that the referring court was "calling into question the Commission's finding, in the Privacy Shield Decision, that the United States ensures an adequate level of protection of personal data transferred from the European Union to that third country, and, therefore, as calling into question the validity of that decision"[143].

Similar to the Safe Harbour Adequacy Decision, the Privacy Shield Adequacy Decision imposed limitations on data protection rights when necessary to comply with national security, law enforcement, or public interest purposes, prioritising such purposes when they conflicted with the data protection rights recognised by the Privacy Shield Adequacy Decision. The Court of Justice of the European Union pointed out that "self-certified United States organisations

[139] *Ibid,* para 62.
[140] *Ibid,* paras. 64 and 65.
[141] *Ibid*.
[142] *Ibid*, para. 159.
[143] *Ibid*, para. 160

receiving personal data from the European Union are bound to disregard the [EU-U.S. Privacy Shield Framework Principles] without limitation where they conflict with the [national security, law enforcement and public interest] requirements and therefore prove incompatible with them"[144]. However, the European Commission, upon analysing U.S. laws, in first place FISA, E.O. 12333 and PPD-28, and the letters received from the U.S. authorities and annexed to the Privacy Shield Adequacy Decision, assessed that such prioritisation was limited to what is strictly necessary to achieve the legitimate objectives, and that there existed effective legal mechanisms to protect individuals' fundamental rights[145].

The exception related to processing for national security, law enforcement, and public interest is one of the important similarities between the Safe Harbour and Privacy Shield frameworks. However, the context is very different. The Safe Harbour framework was adopted in 2000, a few years after the EU passed its first legislative act (Directive 46/96/EC) in an environment where cloud computing, big data technologies, social media, massive data collection, and related data analytics technologies were not yet developed or at least not widespread. At that time, data protection case law was limited within the EU, and legislators, supervisory authorities, and data protection experts were not highly focused on these emerging technologies. Individuals whose data were transferred to the EU were also largely unaware of the impact such technologies had on their right to data protection. Therefore, the limited and inefficient protection provided by the Safe Harbour framework, particularly regarding activities related to national security, law enforcement, and public interest purposes, probably went unnoticed as an issue in 2000 and remained so until 2013 and Mr Snowden's revelations. On the other hand, negotiations between the EU and the U.S. to establish a new data transfer framework began in 2014 under circumstances that were substantially different from those when the Safe Harbour Adequacy Decision was adopted. The context in 2014 was defined by significant technological developments in various areas, including "over-the-top" services like WhatsApp, social media platforms like Facebook, cloud computing services like Amazon Web Services, and email services like Google's Gmail, all provided by U.S.-based companies subject to U.S. surveillance programmes. The disclosure of U.S. surveillance in 2013 provided a clear overview of U.S. intelligence activities, while the Schrems I judgment in 2015 outlined the conditions the data transfer framework needed to meet to comply with EU law requirements. Thus, while it is understandable that the European Commission may not have foreseen the

[144] *Ibid*, para. 164.
[145] Privacy Shield Adequacy Decision, paras. 88, 135 and 140.

future impact of U.S. surveillance on individuals' lives in 2000, the same cannot be said for the deficiencies in the Privacy Shield Adequacy Decision adopted in 2016.

Nonetheless, five years after invalidating the Safe Harbour Adequacy Decision, the Court of Justice of the European Union had to analyse the Privacy Shield Adequacy Decision, taking into consideration the reasons expressed by the European Commission in the Privacy Shield Adequacy Decision and the opposing views of the referring court, to determine whether the adequacy decision in question should be invalidated.

The Court of Justice of the European Union started its assessment of the Privacy Shield Adequacy Decision focusing on Articles 7 and 8 of the Charter, by indicating that it is an obligation of the European Commission to confirm compliance with the mentioned Charter's Articles before adopting an adequacy decision[146]. The Court of Justice of the European Union also emphasised that, there has been an interference with the rights recognised in Charter's Articles 7 and 8 as there has been disclosure of personal data to a third party (public authorities) irrespective "of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference"[147]. Afterwards, the Court proceeded to assess whether the detected interference would meet the requirements specified in Article 52 of the Charter, which states limitations to the rights and freedoms established by the Chart must be defined by law and that "subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others"[148]. In relation to the obligation to define the limitations of fundamental rights in the law, the Court of Justice of the European Union, citing the paragraph 139 of its Opinion 1/15 of 26 July 2017 on the EU-Canada PNR Agreement, remarked that the law implementing such limitations must "define the scope of the limitation on the exercise of the right concerned"[149]. Furthermore, using the same opinion as guideline, with regard to the concept of proportionality, the Court pointed out the necessity of the legislation implementing interferences to "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", especially emphasising that such legislation must

[146] *Ibid*, para 169.
[147] *Ibid*, para 171.
[148] *Ibid,* para. 174.
[149] *Ibid,* para 175.

clarify the conditions and circumstances where a "measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary", concluding that safeguards are especially needed in case of automated data processing[150].

Regarding the requirements explicitly emerging from the General Data Protection Regulation, its Article 45(2)(a) states that the European Commission needs to take into consideration whether the protection provided by a third country ensures that the data subjects whose data are transferred from the EU to the U.S., have "effective and enforceable data subject rights"[151]. The positions of the European Commission and the referring court were visibly opposed. The European Commission expressed in the Privacy Shield Adequacy Decision that "the United States ensures effective legal protection against interferences by its intelligence authorities"[152], while the referring court, pointed out that the redress mechanisms available to EU citizens were insufficient and not comparable to the avenues available to U.S. citizens to enforce their rights, also criticising the role of the Privacy Shield Ombudsperson[153].

In order to determine the compatibility of the U.S. surveillance practices with the EU data protection standards, the Court of Justice of the European Union proceeded to assess whether the legal basis upon which the U.S. authorities carry out its surveillance activities, i.e. the Section 702 of the FISA and on E.O. 12333, limit the processing of personal data in accordance with the principle of proportionality, as guaranteed by the second sentence of Article 52(1) of the Charter[154]. The Privacy Shield Adequacy Decision has stipulated that the FISC authorises surveillance programs, but not individual surveillance activities, leading the Court of Justice of the European Union to remark that "the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information'"[155]. The Court concluded that the "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" and, in line with the Advocate General's

[150] *Ibid*, paras. 175 and 176.
[151] Article 45(2)(a) of the General Data Protection Regulation.
[152] Privacy Shield Adequacy Decision, recital 123.
[153] Schrems II judgment, paras. 64 and 65.
[154] *Ibid*, para. 178.
[155] Privacy Shield Adequacy Decision, recital 109.

opinion, that that provision has not ensured "a level of protection essentially equivalent to that guaranteed by the Charter", as it has not defined "the scope of the limitation on the exercise of the right concerned nor clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards"[156]. With regard to the E.O. 12333, as explicitly confirmed in the recital 115 of the Privacy Shield Adequacy Decision, there were no redress mechanisms available to data subjects, which was also confirmed by the Court stating that the mentioned executive order "does not confer rights which are enforceable against the U.S. authorities in the courts either"[157].

Although the European Commission has celebrated the PPD-28 as a document of "particular importance for non-U.S. persons, including EU data subjects"[158], the Court of Justice of the European Union confirmed that it "does not grant data subjects actionable rights before the courts against the U.S. authorities"[159]. Having considered all these findings, the Court of Justice of the European Union concluded that data subjects whose personal data are transferred to from the EU to the U.S. did not have effective and enforceable rights[160].

Regarding the bulk collection of personal data, such collection is expressly admitted under Section 2 of the PPD-28 which states that "the United States must consequently collect signals intelligence in bulk"[161]. In words of the Court of Justice of the European Union, "that possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, 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"[162].

As expected, considering Section 702 of the FISA and E.O. 12333, read in conjunction with PPD-28, the Court concluded that the "surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary", and that the limitations imposed on the protection of personal data transferred from the EU to the U.S. "are not circumscribed in a

[156] *Ibid*, para. 180.
[157] *Ibid*, para. 182.
[158] Privacy Shield Adequacy Decision, recital 69.
[159] Schrems II judgment, para. 181.
[160] Schrems II judgment, paras. 188-199.
[161] Section 2 of the Presidential Policy Directive -- Signals Intelligence Activities, Policy Directive/PPD-28 of January 17, 2014.
[162] Schrems II judgment, para. 183.

way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter"[163].

Although it was already clear that the Court had sufficient grounds to declare the Privacy Shield Adequacy Decision invalid, it also decided to address the question of the Privacy Shield Ombudsperson.

Thus, the Court of Justice of the European Union directed its attention to Article 47 of the Charter, which imposes the right of individuals to have an effective remedy before an independent and impartial tribunal regarding the rights or freedoms protected by EU law. The General Data Protection Regulation replicates the essence of the aforementioned Charter provision and states in Article 45(2)(a) that one of the criteria for recognising that a third country has an adequate level of protection is the existence of *"*effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred"[164]. In words of the Court of Justice of the European Union, "the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law"[165].

The Privacy Shield Ombudsperson was introduced into the U.S. legal framework, as confirmed by the U.S. Secretary of State in his letter of July 7, 2016 (Annex III to the Privacy Shield Adequacy Decision) and served as a key pillar for the European Commission's argument regarding the adequate level of protection provided by the EU-U.S. Privacy Shield framework. The European Commission, regarding the mentioned ombudsperson mechanism, found "that there are adequate and effective guarantees against abuse"[166], and came to the conclusion that the U.S. "ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU-U.S. Privacy Shield"[167].

In the subsequent points of its judgment, the Court of Justice of the European Union proceeded to assess the European Commission's consideration of the key role of the Privacy Shield Ombudsperson in ensuring the rights guaranteed by Article 47 of the Charter.

[163] *Ibid*, para. 184 and 185.
[164] Article 45(2)(a) of the General Data Protection Regulation.
[165] *Ibid*, para. 187.
[166] Privacy Shield Adequacy Decision, recital 122.
[167] *Ibid*, recital 123.

Repeating the very own words of the European Commission in the recital 115 of the Privacy Shield Adequacy Decision, the Court of Justice of the European Union stated that it is "clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered", and confirms what is obvious, that "the existence of such a lacuna in judicial protection in respect of interferences with intelligence programmes based on that presidential decree makes it impossible to conclude, as the Commission did in the Privacy Shield Decision, that United States law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter"[168].

Besides that, the Court of Justice of the European Union also indicated that the aforementioned Ombudsperson is appointed by the U.S. Secretary of State and forms an integral part of the U.S. State Department, without protection from dismissal or revocation, which could undermine the independence of the individual in that role[169]. The Court remarked that there are no reasons to believe that the Privacy Shield Ombudsperson could adopt binding decisions affecting the intelligence community and noted that there are no tangible legal safeguards on which data subjects could rely[170]. All these findings led the Court of Justice of the European Union to conclude that the redress mechanism in question did not ensure individuals' access to a tribunal that would protect their rights in accordance with Article 47 of the Charter and, therefore, did not meet the guarantees required by that Article[171].

As is clear from the analysis provided by the Court, it decided to invalidate the Privacy Shield Adequacy Decision[172].

The second invalidation of a mechanism for the free flow of personal data from the EU to the U.S. raised many questions at that time, and it was unclear what the future of data transfers would be if the data protection authorities of EU Member States began to enforce the data transfer rules in accordance with the position of the Court of Justice of the European Union. However, considering the strong commercial ties between the U.S. and the EU, as well as the lack of interest in a generalised effective enforcement, the invalidation of the Privacy Shield

[168] Schrems II judgment, para. 191.
[169] *Ibid*, para. 195.
[170] *Ibid*, para. 196.
[171] *Ibid*, para. 197.
[172] *Ibid*, para. 201.

Adequacy Decision—similar to the invalidation of the Safe Harbour Adequacy Decision—has had a very limited effect on the flow of personal data from the EU to the U.S.[173]

In these circumstances, the European Data Protection Board adopted on 10 November 2020 the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[174]. The aim was to guide personal data exporters from the EU when using standard contractual clauses for international data transfers. Although these recommendations were widely consulted by entities exporting personal data from the EU to the U.S., as they could no longer rely on the Privacy Shield Adequacy Decision, data transfers to the U.S. did not significantly suffer. Companies began implementing standard contractual clauses, and in practice, only a small number of international data transfer cases were addressed by the data protection authorities[175]. Therefore, the effect of the Recommendations was limited to warning that standard contractual clauses could be used for data transfers to the U.S., but only in situations where such transfers do not pose a risk to the level of protection provided by those clauses. This is, in principle, impossible, as U.S. laws take precedence over any type of contract between parties involved in data transfers. To address these risks, the Recommendations provide supplementary measures, such as encryption without sharing the encryption key with any entity governed by U.S. law, which need to be implemented alongside the terms defined in the standard contractual clauses[176]. However, these Recommendations also faced unfounded criticism, which claimed that the measures did not cover all cases of data transfers—a claim that is practically impossible to achieve. Additionally, it was argued that there is no distinction between mere access to and the actual transfer of personal data. This

[173] In line with the predictions made by Katulić T. and Vojković G., "From Safe Harbour to European Data Protection Reform", MIPRO 2016, 39th International Convention, 2016, available on https://www.researchgate.net/publication/305046213_From_Safe_Harbour_to_European_Data_Protection_Reform, p. 1697.

[174] 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, version 2.0, adopted on 18 June 2021, available on: https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[175] Naef T., Data Protection without Data Protectionism, The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law, European Yearbook of International Economic Law, EYIEL Monographs - Studies in European and International Economic Law, Springer, Volume 28, 2023, p. 426 and 427, available on https://doi.org/10.1007/978-3-031-19893-9.

[176] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, para. 90.

criticism is misplaced, as the right to protect personal data can also be infringed upon by mere remote access to data[177].

While these Recommendations were adopted to address data transfers conducted under standard contractual clauses, the European Commission and the U.S. authorities continued to seek a transfer framework that would facilitate free data flows[178]. After the data transferring mechanisms were invalidated twice, a key question arises: how can U.S. surveillance activities be addressed? In Murphy's work, she proposes that addressing the lack of proportionality related to generalised surveillance and the collection of personal data, as well as the insufficient safeguards, is much more feasible than calling for the total elimination of U.S. generalised surveillance activities over personal data transferred from the EU[179]. However, achieving this would also require an unexpected change in the position of the Court of Justice of the European Union regarding such massive surveillance and would represent a step back in the level of personal data protection guaranteed by the EU.

Interestingly, almost exactly three years after the invalidation of the Privacy Shield Adequacy Decision, the ongoing bulk collection of personal data under E.O. 12333, performed despite (or in accordance with) the order, did not prevent the European Commission from adopting its third adequacy decision for personal data transfers to the U.S., based on a framework similar to those of both previously invalidated decisions.

8. Third time's the charm: the EU-U.S. Data Privacy Framework Adequacy Decision

On July 10, 2023, the European Commission declared that the EU-U.S. Data Privacy Framework provides an adequate level of protection for personal data transferred from the EU to U.S. companies that are self-certified under this framework. Subsequently, the Commission adopted the relevant adequacy decision. This adequacy decision has the status of an implementing act based on Article 45(3) of the General Data Protection Regulation.

[177] Neiazy V., „Invalidation of the EU–US Privacy Shield: impact on data protection and data security regarding the transfer of personal data to the United States", Int. Cybersecur. Law Rev. 2, 2021, p. 34, available on https://doi.org/10.1365/s43439-021-00018-7.
[178] The EU-U.S. Data Privacy Framework: Background, Implementation, and Next Steps, 24 October 2022, Congressional Research Service, p. 2, available on https://crsreports.congress.gov/product/pdf/LSB/LSB10846.
[179] Murphy M.H., „Assessing the implications of Schrems II for EU–US data flow", International & Comparative Law Quarterly , Volume 71 , Issue 1 , January 2022 , p. 257, available on: https://doi.org/10.1017/S0020589321000348.

After the expected invalidation of the Privacy Shield framework in July 2020, the European Commission proposed a new mechanism that significantly relied on approaches previously invalidated. The inability to create an effective deviation from prior data transfer mechanisms stems from the lack of any substantial changes in the relevant legal framework of the U.S. to ensure alignment with EU data protection standards and the improvement of individuals' rights. This approach can be viewed as risky regarding its sustainability as a valid transfer mechanism, especially considering that transfers to the U.S. face much more public scrutiny than those conducted under adequacy decisions for Israel or Japan, even though both of these countries also engage in extensive surveillance practices.[180].

Meanwhile, in addition to the Schrems II judgment and the Article 29 Data Protection Working Party's Adequacy Referential, the European Data Protection Board issued the Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures after the Schrems II judgment. These recommendations provided additional guidance and clear indications on the standards that a third country's legislation must satisfy to be considered as offering an adequate level of protection for personal data.

However, despite the case law of the Court of Justice of the European Union, the documents issued by EU data protection authorities, and the lack of substantial changes in U.S. legislation regarding the processing of personal data for national security and law enforcement activities, the European Commission decided to proceed with authorising data transfers under the third mechanism for transferring personal data to the U.S., namely the EU-U.S. Data Privacy Framework. This approach was likely influenced by the potential impact that limitations on data transfers to the U.S. could have on business activities, as highlighted in various documents and joint statements discussing the business connections between these two jurisdictions[181]. The most practical instrument for carrying out international transfers is adequacy decisions, as these do not require any additional action from the entities involved in the data transfers. However, there is a very limited number of countries with such adequacy decisions. In contrast, other transfer mechanisms, such as standard contractual clauses, are widely used for transfers to third countries, although their implementation is not always appropriate. As described in the

[180] Juliussen B. A., Kozyri E., Johansen D., Rui J. P., "The third country problem under the GDPR: enhancing protection of data transfers with technology", International Data Privacy Law, Volume 13, Issue 3, August 2023, available on https://doi.org/10.1093/idpl/ipad013, p. 229.
[181] For example, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 and https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, the commonly used standard contractual clauses defined in Article 46(1)(b) of the General Data Protection Regulation may not be suitable for data transfers at all, due to the lack of appropriate supplementary measures needed to protect the transferred personal data[182]. It is important to consider that the role of these supplementary measures, which consist of technical and organisational instruments, is to reinforce the standard contractual clauses (essentially a contract between the data exporter and the data importer) against the primacy of the legal framework of a third country where the data is exported, particularly in cases where that framework undermines the data protection rules agreed upon in the standard contractual clauses. Despite the fact that appropriate technical measures, such as the bring-your-own-key approach, are not always feasible to implement, adequacy decisions permitting transfers to third countries could help fill these gaps and be utilised in all cases. Nevertheless, while such adequacy decisions are legally sound and satisfactory for entities transferring personal data, they do not always provide effective protection for fundamental rights, as demonstrated by the Court of Justice of the European Union in its judgments invalidating the Safe Harbour and Privacy Shield adequacy decisions.

As stated by the European Commission in point 6 of the EU-U.S. Data Privacy Framework Adequacy Decision, following the Court's invalidation of the Privacy Shield adequacy decision in the Schrems II judgment, the Commission and the U.S. government began negotiations to establish a new framework for data transfers based on a fresh adequacy decision. Consequently, on 7 October 2022, the U.S. adopted Executive Order 14086, titled "Enhancing Safeguards for U.S. Signals Intelligence Activities" (hereinafter: E.O. 14086)[183], which was further complemented by a Regulation on the Data Protection Review Court issued by the U.S. Attorney General[184]. This new executive order aimed to strengthen safeguards to ensure that data principles are substantially equivalent to those outlined in EU law. Nevertheless, E.O. 14086 essentially promotes proportionality without amending U.S. legislation, which has previously been found to conflict with EU data protection standards. As a result, this approach

[182] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, p. 4.
[183] Executive Order 14086 of October 7, 2022 "Enhancing Safeguards for United States Signals Intelligence Activities", available on https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.
[184] EU-U.S. Data Privacy Framework Adequacy Decision, recital 6.

jeopardises the stability of the framework and raises the risk of further invalidation[185]. Additionally, the substantive definitions outlined in the executive order are not compatible with the interpretations of these definitions provided by the Court of Justice of the European Union[186].

As with the invalidated Safe Harbour and Privacy Shield mechanisms, not all data transfers from the EU to the U.S. are covered by the rules of the EU-U.S. Data Privacy Framework. This is because only U.S. organisations subject to the investigatory and enforcement powers of the Federal Trade Commission or the U.S. Department of Transportation, that have completed the self-certification process and committed to implementing a set of personal data protection measures (the "EU-U.S. Data Privacy Framework" along with the Supplemental Principles) issued by the U.S. Department of Commerce, are eligible to receive personal data from the EU without having to meet any other conditions. The self-certification process must be performed on annual basis[187].

The EU-U.S. Data Privacy Framework aims to ensure the application of data protection principles that are comparable to those defined by previous data transfer mechanisms. These principles include notice (transparency), choice (the right to opt in or opt out), accountability for onward transfers, security, data integrity, purpose limitation, access, recourse, enforcement and liability, data accuracy, minimisation, transparency, and onward transfer protection[188].

The U.S. Department of Commerce is responsible for administering and monitoring compliance with the EU-U.S. Data Privacy Framework, while enforcement activities are carried out by the Federal Trade Commission and the Department of Commerce, acting as independent supervisory authorities with the necessary investigatory and enforcement powers[189]. More specifically, under the framework, the Federal Trade Commission oversees compliance and can enforce it by seeking administrative or federal court orders, among other remedies. If a company fails to adhere to an order from the Federal Trade Commission, the commission may impose civil penalties and other corrective measures, including compensation for any harm caused by

[185] Juliussen B. A., Kozyri E., Johansen D., Rui J. P., "The third country problem under the GDPR: enhancing protection of data transfers with technology", International Data Privacy Law, Volume 13, Issue 3, August 2023, available on https://doi.org/10.1093/idpl/ipad013, p. 230.
[186] Ortega Giménez, A. "¿Y a la tercera va la vencida?. El nuevo marco transatlántico de privacidad de datos UE-EE.UU.", *Cuadernos de Derecho Transnacional*, 16(1), 2024, available on: https://doi.org/10.20318/cdt.2024.8432, pp. 501.
[187] EU-U.S. Data Privacy Framework Adequacy Decision , recital 9.
[188] *Ibid,* title 2.2.
[189] *Ibid,* title 2.3.4.

non-compliance[190]. In addition, the U.S. Department of Transportation monitors airline compliance and, in collaboration with the Federal Trade Commission, supervises the data protection practices of ticket agents involved in air transportation sales[191].

Regarding the redress rights of data subjects whose personal data have been transferred under this adequacy decision, individuals are entitled to lodge complaints related to non-compliance[192]. They can submit a complaint directly to the organisation, to an independent dispute resolution body designated by the organisation, to a national EU supervisory authority, the U.S. Department of Commerce, or the Federal Trade Commission. Additionally, individuals have the right to seek a binding arbitration decision[193].

It is evident that the characteristics of the data protection rules governing transfers from the EU to the U.S. under this new mechanism, including the U.S.'s specific approach based on self-certification, do not offer an identical level of protection (which is not a requirement). However, it cannot be said that these characteristics fail to meet the requirement of ensuring a "level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the [General Data Protection Regulation], read in the light of the Charter"[194].

a. Data processing for law enforcement purposes

The personal data transferred to self-certified organisations may be accessed by U.S. authorities for law enforcement purposes.

In the first instance, at the request of a federal law enforcement officer or a government attorney, a judge may issue a warrant for a search or seizure (including electronically stored information) if the necessary procedural and factual conditions are satisfied[195]. Additionally, a grand jury can issue subpoenas requiring individuals or entities to produce or make available items such as business records or electronically stored information, while public authorities in the U.S. can also issue administrative subpoenas, in accordance with the law, to access data held by companies for civil or regulatory purposes[196]. Finally, several legal bases allow criminal law

[190] *Ibid*.
[191] *Ibid*.
[192] *Ibid*, recital 68.
[193] *Ibid*.
[194] Schrems II judgment, para 94.
[195] EU-U.S. Data Privacy Framework Adequacy Decision, recital 92.
[196] Schrems II judgment, paras. 93 and 94.

enforcement authorities to gain access to communications data, provided they obtain a court order[197].

Regarding the oversight of personal data processing for law enforcement purposes, the European Commission, in the EU-U.S. Data Privacy Framework Adequacy Decision, highlights the initial oversight by courts when authorising the collection of transferred personal data under the framework. Additionally, certain roles are identified as having oversight functions. These include the Privacy and Civil Liberties Officers, appointed within various departments responsible for criminal law enforcement, and the Inspectors General[198]. However, it is important to note that both of these are roles within their respective administrative bodies, rather than fully independent entities[199]. Finally, concerning counter-terrorism activities conducted by law enforcement agencies, oversight is provided by the Privacy and Civil Liberties Oversight Board, which is established as an independent agency within the executive branch[200]. This Board is composed of five bipartisan members appointed by the President for a fixed six-year term, subject to Senate approval[201].

Data subjects whose personal data have been transferred under the EU-U.S. Data Privacy Framework Adequacy Decision may submit requests or complaints to criminal law enforcement authorities regarding the handling of their personal data[202]. This includes requests for access to and correction of their personal data, as well as seeking judicial redress against public authorities or their officials[203]. This includes protection under the Administrative Procedure Act, which allows recipients of administrative subpoenas to challenge them in court on the grounds that they are unreasonable, such as being overly broad, oppressive, or burdensome[204].

However, a noticeable discrepancy between the data protection frameworks in the EU and the U.S. concerns the powers of national security authorities and the limitations faced by data subjects in exercising their data protection rights when their data is transferred from the EU to the U.S.

[197] EU-U.S. Data Privacy Framework Adequacy Decision, recitals 95-98.
[198] *Ibid*, recitals 108-109.
[199] *Ibid*.
[200] *Ibid*, recital 110.
[201] *Ibid*.
[202] *Ibid, recital 113.*
[203] *Ibid*, recitals 113 and 114.
[204] *Ibid*, recital 112.

b. Data processing for national security purposes

U.S. laws provide numerous avenues that facilitate extensive processing of personal data for national security purposes, including the collection of such data outside U.S. borders in certain circumstances. The mechanisms available to non-U.S. individuals for protecting their rights before U.S. authorities differ significantly from those accessible within the EU.

As a general rule, when personal data is transferred to the U.S., local national security authorities are authorised to request access to such data from companies under the powers granted by FISA or through National Security Letters (NSL)[205]. Additionally, under E.O. 12333, intelligence agencies have the capacity to collect personal data outside the U.S., which may include data in transit between the EU and the U.S. before it enters U.S. territory (for example, by intercepting undersea telecommunications cables)[206].

The EU-U.S. Data Privacy Framework Adequacy Decision mainly relies on the expectations that it will endure in the future based on the U.S. President-issued E.O. 14086. Considering that previous data transfer mechanisms have been invalidated due to the extensive powers granted to U.S. national security authorities, the aim of the mentioned executive order is to limit those powers and provide effective rights to EU data subjects whose data have been transferred from the EU to the U.S.

As the European Commission states in recital 124 of the EU-U.S. Data Privacy Framework Adequacy Decision, the executive order replaces many provisions of PPD-28 and "strengthens the conditions, limitations, and safeguards that apply to all signal intelligence activities", covering data collection activities performed under FISA and E.O. 12333[207]. The E.O. 14086 establishes a new redress mechanism through which these safeguards can be invoked and enforced by individuals.

The level of admiration the European Commission had previously expressed for PPD-28, almost regarding it as the backbone of data protection that ensures full compliance of U.S. processing activities for national security purposes with high EU data protection standards[208], has now been knocked-down by the introduction of E.O. 14086, which is considered to be the new guarantor of data protection rights within the U.S. national security framework.

[205] *Ibid*, recital 121.
[206] Schrems II judgment, para. 63.
[207] *Ibid*, recital 124.
[208] For example, see Privacy Shield Adequacy Decision, recitals 69 and 74.

However, not all PPD-28 provisions have cessed to apply, more precisely sections 3 and 6 remain in force. The section 3 states that "signals intelligence collection raises special concerns, pointing out the unique nature of such collection and the inherent concerns raised when signals intelligence can only be collected in bulk. It remarks the obligation of national security policymakers [to] consider carefully the value of signals intelligence activities, and prescribes that the heads of departments and agencies that participate in the policy processes for establishing signals intelligence priorities and requirements shall, on an annual basis, review any priorities or requirements identified by their departments or agencies"[209]. Simultaneously, the section 6 that also remains applicable, prescribes that it does not affect "the authority or responsibility granted by law to a United States Government department or agency"[210]. From the content of the surviving provisions, it can be concluded that they do not constitute a significant source of individuals' data protection rights. Furthermore, it confirms that there are situations in which bulk collection of data occurs, and these provisions cannot override any activities carried out in accordance with the law.

The E.O. 14086 seeks to ensure a higher level of privacy protection than the one guaranteed by the PPD-28. Intelligence agencies in the U.S. must apply the standards set by E.O. 14086 when selecting or identifying categories of foreign intelligence information to be acquired pursuant to Section 702 of the FISA, collecting foreign intelligence or counterintelligence pursuant to E.O. 12333, and making individual targeting decisions under Section 702 of the FISA and E.O. 12333[211].

As pointed out by the European Commission in recital 126 of the EU-U.S. Data Privacy Framework Adequacy Decision, E.O. 14086 needed to be further implemented in the policies and procedures of national security authorities that regulate their day-to-day operations[212]. They have been required to bring those internal rules in line with the executive order's requirements by a deadline of one year (i.e. by 7 October 2023)[213].

[209] Section 3 of the Presidential Policy Directive -- Signals Intelligence Activities, Policy Directive/PPD-28 of January 17, 2014.
[210] *Ibid,* section 6.
[211] EU-U.S. Data Privacy Framework Adequacy Decision, recital 125.
[212] *Ibid*, recital 126.
[213] *Ibid.*

In essence, the EU 14086 has repeated the already existing approach upon which intelligence activities "must be based on statute or Presidential authorisation and undertaken in compliance with U.S. law, including the Constitution"[214].

The European Commission has assessed in recital 131 that the cited wording introduces the obligation to seek a balance between privacy, civil liberties, and intelligence activities[215]. For this conclusion, the European Commission relies on Section 2(a)(ii)(B) of that executive act, which states:

> "signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside"[216].

Considering the necessity to balance between intelligence necessities and data protection rights, the E.O. 14086 stipulates what can be a legitimate objective of intelligence activities and what must never be pursued by intelligence activities.

Regarding legitimate objectives, the E.O. 14086 outlines twelve points, some of which are described quite generally[217]. In the EU-U.S. Data Privacy Framework Adequacy Decision, the European Commission mentions only a few of these as examples, such as protecting against foreign military capabilities and activities or assessing transnational threats that impact global security. In terms of forbidden objectives, these include actions that burden criticism, dissent, or the free expression of ideas or political opinions by individuals or the press; disadvantage individuals based on their ethnicity, race, gender, gender identity, sexual orientation, or religion; or provide a competitive advantage to U.S. companies[218].

Describing how the legitimate objectives are implemented in practice, in recital 135 of the EU-U.S. Data Privacy Framework, the European Commission states that intelligence priorities are initially designed by the Director of National Intelligence through the National Intelligence

[214] *Ibid*, recital 128.
[215] *Ibid,* recital 131.
[216] Section 2(a)(ii)(B) of the Executive Order 14086 of October 7, 2022 "Enhancing Safeguards for United States Signals Intelligence Activities".
[217] *Ibid,* Section 2(b)(i)(A).
[218] EU-U.S. Data Privacy Framework Adequacy Decision, recital 134.

Priorities Framework and submitted to the U.S. President for approval[219]. The European Commission also highlights the role of the Civil Liberties Protection Officer of the Office of the Director of National Intelligence. This officer is responsible for providing an assessment for each intelligence priority, indicating whether it relates to one or more legitimate objectives, whether it does not aim at achieving prohibited objectives, and whether the privacy and civil liberties of all affected persons have been properly considered[220]. Although the Civil Liberties Protection Officer's perspective is not decisive, if the Director of National Intelligence disagrees with it, both positions must be presented to the President[221].

Furthermore, the European Commission describes the scope and impact of data collection in "bulk" and analyses E.O. 12333 as the basis for such collection outside U.S. borders[222]. Although E.O. 14086 prioritises targeted collection, this limitation is merely a principle rather than a set of strict rules clearly restricting bulk collection activities[223].

The EU-U.S. Data Privacy Framework Adequacy Decision describes the safeguards applicable to bulk collection. Firstly, the European Commission remarks on a limitation related to data quality, stating that relevant measures should be in place to ensure that the data is collected "only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information"[224]. Secondly, it is indicated that the limits for "use of information collected in bulk (including querying) to six specific objectives, including protecting 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"[225]. Finally, the EU-U.S. Data Privacy Framework Adequacy Decision notes that the E.O. 14086 implements the obligation to establish an assessment that should ensure that the "impact of the queries on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside is taken into account"[226].

---

[219] *Ibid*, recital 135
[220] *Ibid.*
[221] *Ibid.*
[222] *Ibid*, recital 141.
[223] Section 2(b)(ii)(A) of the Executive Order 14086 of October 7, 2022 "Enhancing Safeguards for United States Signals Intelligence Activities".
[224] EU-U.S. Data Privacy Framework Adequacy Decision, recital 141.
[225] *Ibid.*
[226] *Ibid*.

As one of the additional safeguards, the European Commission considers the obligation to submit annual certification to the FISC; however, it is not entirely clear how that court helps to efficiently protect the rights of individuals whose personal data are transferred to the U.S. In this context, it is important to mention that the FISC is an independent tribunal created by federal statute, whose decisions can be appealed to the Foreign Intelligence Surveillance Court of Review and, ultimately, the Supreme Court of the U.S. The FISC certifies that the surveillance programmes are aligned with FISA; however, individual targeting determinations are made by the NSA which is the intelligence agency responsible for targeting under Section 702 of the FISA, being this individual targeting not subject to previous judicial authorisation[227]. Therefore, while the FISC issues annual certifications for surveillance activities, it does not receive a rationale for the targeting of individuals. Consequently, the role of the FISC is to review the certifications and the related procedures (in particular, targeting and minimisation procedures) for compliance with the requirements of FISA, indicating that the role of the FISC remains the same as under the rules of the invalidated Privacy Shield Adequacy Decision[228]. Moreover, the FISC also authorises the installation of pen registers or trap and trace devices on an individualised basis[229].

Regarding the role of the FISC, in the already cited Report from 2013, it was indicated that the "FISC operates ex parte and in camera. Its orders and opinions are classified, unless they are declassified. There is no judicial oversight of the collection of foreign intelligence outside the U.S. under Executive Order 12333, which are conducted under the sole competence of the Executive Branch"[230].

However, regarding E.O. 12333, there are changes brought by the EU-U.S. Data Privacy Framework Adequacy Decision. The E.O. 14086, complemented by the Attorney General Regulation establishing the Data Protection Review Court (an independent tribunal consisting of at least six judges elected for a renewable four-year term), enables the newly established court to handle and resolve complaints from individuals concerning U.S. signals intelligence activities, including activities covered by the E.O. 12333[231].

[227] *Ibid*, recitals 143-145.
[228] Privacy Shield Adequacy Decision, recital 109.
[229] EU-U.S. Data Privacy Framework Adequacy Decision, recitals 151.
[230] Report from 2013, p. 18.
[231] EU-U.S. Data Privacy Framework Adequacy Decision, recitals 124 and 185.

As already stated in the invalidated Privacy Shield Adequacy Decision[232], NSLs also serve as basis for accessing personal data transferred to U.S. companies. As described in EU-U.S. Data Privacy Framework Adequacy Decision's recital 153, NSLs are "authorised by different statutes and allow investigating agencies to obtain certain information (not including the content of communications) from certain entities (e.g. financial institutions, credit reporting agencies, electronic communication providers) contained in credit reports, financial records and electronic subscriber and transactional records"[233]. Regarding electronic communications, based on 18 U.S. Code, section 2709, titled "Counterintelligence access to telephone toll and transactional records", "access to electronic communications may be used only by the FBI and requires that requests use a term that specifically identifies a person, entity, telephone number, or account and certify that the information is relevant to an authorized national security investigation to protect against international terrorism or clandestine intelligence activities"[234]. The cited section does not require a court order for such access, although the mentioned recital of the EU-U.S. Data Privacy Framework Adequacy Decision states that the "recipients of an NSL have the right to challenge it in court"[235].

Regarding the further use of the collected personal data, the European Commission described the relevant safeguards under a separate title[236]. However, the content is focused on safeguards implemented by the intelligence agencies in the U.S. that, in essence, do not differ from the approach commonly adopted in the intelligence community globally. In describing these additional safeguards, it is noted that each intelligence agency must ensure appropriate data security and prevent access by unauthorised persons to personal data collected through signals intelligence. One cannot help but question why this would be deemed a data protection achievement, considering that intelligence agencies (also widely known as secret services), even in countries that are subject to global sanctions for human rights violations, keep the information they collect as "secret" and accessible only to a very narrow scope of vetted personnel. Additionally, the decision remarks upon the obligation to ensure data quality and objectivity when performing intelligence analysis, which certainly should not be especially highlighted, as both values are necessary to make effective decisions, and not solely to respect individuals' data protection rights, but also to manage intelligence resources effectively. Data

[232] Privacy Shield Adequacy Decision, recital 78.
[233] EU-U.S. Data Privacy Framework Adequacy Decision, recitals 153.
[234] 18 U.S. Code, section 2709.
[235] EU-U.S. Data Privacy Framework Adequacy Decision, recitals 153.
[236] *Ibid*, recitals 154-160.

retention is also mentioned as one of the additional safeguards; however, no specific deadlines for data deletion are specified, and it is only stated that the authorities need to implement the appropriate retention periods "laid down in different legal instruments"[237]. Certainly, a positive additional safeguard is the obligation of each intelligence agency to keep appropriate documentation about the collection of signals intelligence to, among other purposes, "facilitate oversight of compliance with the applicable legal requirements as well as effective redress"[238].

c. Oversight on the surveillance activities

One of the most important aspects to assess regarding the protection of personal data collected and further processed by the state, particularly by national security authorities, is the oversight mechanisms that ensure compliance with the law. Effective oversight mechanisms serve to verify whether personal data processing adheres to applicable legal requirements, but do not guarantee that the laws or other legal sources, such as executive orders, provide a level of data protection that is "essentially equivalent to that guaranteed within the European Union by virtue of the [General Data Protection Regulation], as interpreted in light of the Charter"[239].

In the EU-U.S. Data Privacy Framework Adequacy Decision the European Commission dedicates the section 3.2.2. to the oversight of data processing activities performed for national security purposes.

In the mentioned section, it is noted that E.O. 14086 requires each intelligence agency to appoint senior-level legal, oversight, and compliance officials to ensure adherence to applicable U.S. law[240]. This oversight function is carried out by officers with designated compliance roles, as well as by Privacy and Civil Liberties Officers[241]. The responsibilities of these officers include ensuring that relevant procedures are in place and that individuals' complaints are properly addressed. In addition to these roles, each intelligence agency has an independent Inspector General who is responsible, among other duties, for overseeing foreign intelligence activities[242]. This includes oversight within the Office of the Director of National Intelligence and the Office

[237] *Ibid*, recital 157.
[238] *Ibid*, recital 159.
[239] Schrems II judgment, para. 94.
[240] Section 3.2.2. of the EU-U.S. Data Privacy Framework Adequacy Decision
[241] *Ibid*, recital 164.
[242] *Ibid*, recital 165.

of the Inspector General of the Intelligence Community, which has the authority to supervise the activities of the intelligence community and investigate any suspected unlawful conduct[243].

Additionally, one of the oversight mechanisms is the Intelligence Oversight Board, which is established within the President's Intelligence Advisory Board[244]. It is important to note that this board possesses only advisory powers.

In the same section, the oversight body mentioned is the Privacy and Civil Liberties Oversight Board, which is an independent agency consisting of five members appointed by the President for a fixed six-year term, with Senate approval[245]. The role of this Board is to protect privacy and civil rights in the field of counterterrorism. It also has specific functions regarding the implementation of E.O. 14086, particularly by reviewing whether the procedures of the intelligence community are consistent with that executive order and by evaluating the proper functioning of the redress mechanism.

Interestingly, under this section of the EU-U.S. Data Privacy Framework Adequacy Decision, the European Commission, as it did in the Privacy Shield Adequacy Decision, also highlights the role of specific committees in the U.S. Congress, namely the House and Senate Intelligence and Judiciary Committees[246]. However, these committees represent a form of political oversight and cannot be considered in any way as expert data protection authorities that are independent from political influence and focused exclusively on the protection of personal data.

Lastly, the previously mentioned FISC has also been pointed out as one of the oversight bodies[247]. However, as has been noted, the FISC issues annual certifications for surveillance activities and does not receive a rationale for targeting specific individuals. Therefore, the role of the FISC is limited to reviewing the certifications and the related procedures (in particular, targeting and minimisation procedures) for compliance with the requirements of FISA[248]. The role of the FISC also relates to the obligation of compliance officers in U.S. intelligence agencies to report any violations of Section 702 of the FISA related to targeting, minimisation,

[243] *Ibid*.
[244] *Ibid*, recital 166.
[245] *Ibid*, recital 167.
[246] *Ibid*, recitals 168-171.
[247] *Ibid*, recital 173.
[248] The scope has not change in comparison to the one described in recital 109 of the Privacy Shield Adequacy Decision.

and querying procedures to the Department of Justice and the Office of the Director of National Intelligence, which, in turn, report these violations to the FISC[249].

As a unified conclusion, we can state that although many different mechanisms have been described in Section 3.2.2 of the EU-U.S. Data Privacy Framework, none of these roles can substantially compare to the independent authorities mentioned in Article 8(3) of the Charter and Article 45(2)(b) of the General Data Protection Regulation.

d. Individuals' right to redress

The individuals' right to seek redress is one of the essential elements for assessing whether a country has an adequate level of data protection that is substantially comparable to that in the EU, as explicitly stated in Article 45(2)(a) of the General Data Protection Regulation[250].

In line with this, before the General Data Protection Regulation was adopted, the Court of Justice of the European Union, in the Schrems I judgment, had already concluded that it is crucial for individuals to have available legal remedies to access their personal data or to obtain the rectification or erasure of such data. The Court remarked that, without these remedies, the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter, would not be satisfied[251]. Afterwards, the Court of Justice of the European Union in Schrems II judgment remarked that "according to settled case law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, 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 her, 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"[252]. Therefore, one of the crucial objectives of the newly negotiated EU-U.S. Data Privacy Framework was certainly related to addressing the lack of effective judicial review that existed in the previous data transfer mechanisms. Without a satisfactory solution aligned with the strict standards set in Article 47 of the Charter, it could be expected that the third data transfer agreement between the EU and the U.S. would be invalidated. Consequently, the European Commission, in the EU-U.S. Data Privacy Framework Adequacy Decision, points out the relevant redress procedures available for individuals whose personal data are transferred under

[249] *Ibid*, recital 173.
[250] Article 45(2)(a) of the General Data Protection Regulation.
[251] Schrems I judgment, para. 95.
[252] Schrems II judgment, para. 187.

the EU-U.S. Data Privacy Framework. It highlights that these redress mechanisms enable individuals to access their personal data, have the lawfulness of government access to their data reviewed, and, if a violation is found, to have such a violation remedied, including through the rectification or erasure of their personal data[253]. The redress mechanisms under U.S. law are also extended to activities regarding signals intelligence under E.O. 12333 (as opposed to the exclusion of the E.O. 12333 from such redress under the Privacy Shield[254]).

The redress process under the currently valid transfer mechanism would be initiated by any individual whose data has been transferred from the EU to the U.S. under the adequacy decision in question[255]. This individual would submit a complaint concerning an alleged violation of U.S. law governing signals intelligence activities. Such a complaint needs to be lodged with a data protection supervisory authority in an EU Member State that is competent for overseeing the processing of personal data by public authorities[256]. Upon receiving the complaint, the competent supervisory authority will channel it, via the secretariat of the European Data Protection Board, to the redress mechanism[257].

The initial investigation of complaints to this redress mechanism is carried out by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence[258]. This officer determines whether a violation of applicable law has occurred and, if that is the case, decides on an appropriate remediation, being the decision binding on intelligence agencies concerned[259]. The redress process always concludes with the same statement, which reads as follows: "the review either did not identify any covered violations or the ODNI CLPO issued a determination requiring appropriate remediation"[260]. As explanation, the European Commission has stated that that approach "allows protection of the confidentiality of activities conducted to protect national security, while providing the individuals with a decision confirming that their complaint has been duly investigated and adjudicated"[261]. In case the individual or an "element of the Intelligence Community" is unsatisfied with the received answer, the individual or the mentioned "element" have the right to challenge such decision to

[253] EU-U.S. Data Privacy Framework Adequacy Decision, para. 181.
[254] Privacy Schield Adequacy Decision, recital 115.
[255] EU-U.S. Data Privacy Framework Adequacy Decision, para. 177.
[256] *Ibid*.
[257] *Ibid*.
[258] *Ibid*, para. 179.
[259] *Ibid*, paras. 179 and 181.
[260] *Ibid*, recital 183.
[261] *Ibid.*

the Data Protection Review Court, for a review[262]. The Data Protection Review Court reviews the complaints in panels of three judges, with the assistance of a Special Advocate, whose role is to ensure that the complainant's interests are represented and that the reviewing court is well informed about all relevant issues of law and facts[263]. When concluding its review, the reviewing court may, by majority voting, (1) decide that there is no evidence indicating that signals intelligence activities occurred involving the personal data of the complainant; (2) determine that the Civil Liberties Protection Officer at the Office of the Director of National Intelligence's determinations were legally correct and supported by substantial evidence; or (3) if it disagrees with the determinations of that officer, issue its own determinations[264]. The final conclusion of the Data Protection Review Court delivered to the individual who has asked for a case review, always reads as follows: "the review either did not identify any covered violations or the DPRC issued a determination requiring appropriate remediation"[265].

Considering that the entire process is classified, the only information to which individuals have access is the information they provide, as well as any questions received from the Special Advocate during the review process. Aside from this, access to the substance of the case can only be achieved if the information pertaining to a review is declassified. If this occurs, the individual will be notified that such information may be available under the U.S. Freedom of Information Act[266]. Due to the limitations imposed on individuals regarding the resolution of their requests, concerns arise about whether the final resolution of complaints can be considered to have "effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred" as required by Article 45(2)(a) of the General Data Protection Regulation[267].

Besides the mentioned redress mechanism through the Civil Liberties Protection Officer of the Office of the Director of National Intelligence in the first instance, and the Data Protection Review Court in the second instance, as established under E.O. 14086, there are more redress mechanisms available before ordinary U.S. Courts under certain conditions[268]. Access to these avenues is subject to the showing of "standing" which, in these cases, as already problematised

[262] *Ibid*, recitals 183 and 184.
[263] *Ibid*, recital 188.
[264] *Ibid*, recitals 190 and 191.
[265] *Ibid*, recital 192.
[266] *Ibid*, recital 193.
[267] Article 45(2)(a) of the General Data Protection Regulation.
[268] EU-U.S. Data Privacy Framework Adequacy Decision, recitals 115 and 199.

in recital 115 of the Privacy Shield Adequacy Decision[269], can hardly be demonstrated, as almost all activities carried out by the U.S. authorities for national security purposes are classified. In order to show standing, it is required to have suffered an "injury in fact" to demonstrate a causal connection between the injury and the conduct challenged, and to show that a favourable decision by the court will address the injury[270]. Specifically, in the adequacy decision in question, the European Commission remarks that under FISA and the related statute, data subjects have the right to bring a civil action for monetary damages against the U.S. when information about them has been unlawfully and wilfully used or disclosed[271]. They can also sue U.S. government officials acting in their personal capacity for monetary damages[272].

Based on the mentioned redress avenues, the European Commission found that there are safeguards which individuals can invoke to enjoy effective redress rights[273].

9. Possible grounds for invalidating the EU-U.S. Data Privacy Framework Adequacy Decision

The first attempt to invalidate the EU-U.S. Data Privacy Framework Adequacy Decision was initiated by French MEP Philippe Latombe. Mr Latombe's main arguments were related to inadequate guarantees for protecting private and family life, considering the widespread collection of personal data in bulk, the lack of effective and independent redress mechanisms available to data subjects, insufficient measures to protect personal data concerning automated decision-making activities on the U.S. side, and the absence of precise data security obligations[274]. The General Court, however, decided to dismiss the application for interim measures, concluding that the applicant did not establish the existence of serious and irreparable harm justifying the urgency of the requested interim measures[275].

As we can see, Mr Latombe decided to approach the General Court instead of a national court of an EU Member State, which would then submit a request for a preliminary ruling to the Court of Justice of the European Union if the conditions were met. In the cases of Schrems I and

[269] Privacy Shield Adequacy Decision, recital 115.
[270] EU-U.S. Data Privacy Framework Adequacy Decision, recital 195 and the related footnote.
[271] *Ibid*, recital 196.
[272] *Ibid*.
[273] *Ibid*, recital 200.
[274] T-553/23, *Latombe v Commission*, Application of 6 September 2023.
[275] T-553/23 R, *Latombe v Commission*, Order of the President of the Court of 12 October 2023 (*Ordonnance)*, para. 29.

Schrems II, Mr Schrems chose the second approach, which, while not as rapid as Mr Latombe's, has proven to be effective.

We will now proceed to analyse the major deficiencies of the EU-U.S. Data Privacy Framework that could be exploited with the aim of invalidating the aforementioned decision.

a. Bulk collection and further processing of personal data

One of the concerns related to the activities acknowledged by the European Commission under the EU-U.S. Data Privacy Framework Adequacy Decision pertains to the bulk collection of personal data processed within internet and telecommunication traffic.

Bulk collection interferes with the fundamental right to privacy, regardless of whether the processed personal data is of a sensitive nature or not, or whether the individuals concerned have experienced any inconvenience[276], and such interference must be carried out in accordance with Article 52(1) of the Charter, which specifies that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others[277].

The Data Retention Directive was invalidated for similar bulk collection practices as the ones performed by the U.S. authorities. When the Court of Justice of the European Union invalidated that directive, it paid attention to the facts that the individuals whose data were retained did not necessarily have any kind of connection to the situation which is liable to give rise to criminal prosecutions[278], and that the invalidated Data Retention Directive failed to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their further use[279]. Therefore, by analogy, in addition to the necessary connection between individuals whose data are retained and the criminal prosecution, the law of the third country imposing such measures should establish objective criteria for determining the limits of access by the competent national authorities to the data and their subsequent use for the purposes of prevention, detection, or criminal prosecution concerning offences. This analogy is essential because personal data should enjoy the same level of

[276] *Digital Rights Ireland and Others*, para. 33.
[277] Article 52(1) of the Charter.
[278] *Ibid*, para. 58.
[279] *Ibid*, para. 60.

protection when transferred to a country or international organisation that has been declared to provide an adequate level of protection. International transfers of personal data under adequacy decisions must not lead to a decrease in the level of protection individuals enjoy in the EU concerning the processing of their personal data.

After that judgment, the Court of Justice of the European Union has further enriched its case law related to bulk collection of data. In the *Tele2 Sverige* judgment, the Court of Justice of the European Union reaffirmed that accessing all retained data—regardless of whether there is a connection—is not limited to what is strictly necessary[280]. The Court held that national legislation must provide objective criteria for granting access to such data by national authorities. However, it opened the door to a more flexible approach, recognising that particular situations—such as threats to national security, defence, or public security posed by terrorist activities—might justify access to data of individuals without any link, even indirect, to the fight against serious crime. The Court added that access to the retained data of such individuals "might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities"[281]. Furthermore, the Court of Justice of the European Union declared that, except in cases of urgency, the access to data carried out by the national authorities should "be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted"[282]. These authorities that have been granted access to the retained personal data must notify the affected individuals once there is no longer any risk to the outcome of the investigation. This notification is necessary to ensure that these individuals can seek legal redress if they believe their rights and freedoms have been infringed[283].

More recently, in the *Privacy International* case, the Court of Justice of the European Union provided further clarifications, when answering if the transmission of traffic data (i.e. any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof) and location data from electronic communication services to security and intelligence agencies for the purpose of safeguarding

[280] C-203/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, judgment of 21 December 2016, ECLI:EU:C:2016:970.
[281] *Ibid*, para. 119.
[282] *Ibid*, para. 120.
[283] *Ibid*, para. 121.

national security is permitted[284]. In that case the Court of Justice of the European Union clarified that, based on Article 15(1) of Directive 2002/58/EC[285], Member States can adopt legislative measures of exceptional appliance, providing for the retention of data for a limited period where this constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system[286]. However, the Court of Justice of the European Union emphasised that the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of that data, explicitly laid down in Article 5 of that directive, cannot become the rule, and that the exception must remain an exception[287]. The Court has specified which standards must meet the national legislation adopted pursuant the Directive 2002/58/EC, remarking that such exceptional legislative rules "must be legally binding under domestic law and, in particular, must 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"[288]. Furthermore, the Court of Justice of the European Union concluded that "national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society"[289].

Besides the above mentioned cases related to the invalidated Data Retention Directive, as already cited, in Schrems II judgment the Court of Justice of the European Union stated that a possibility, "which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial

[284] C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, judgment of 6 October 2020, ECLI:EU:C:2020:790, para 50.
[285] 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) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11)
[286] *Privacy International*, para 58.
[287] *Ibid*, paras. 59 and 69.
[288] *Ibid*, para. 68.
[289] *Ibid*, para. 81.

review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data"[290].

After analysing the Court of Justice of the European Union's case law related to the bulk collection of personal data, it is essential to examine the practices permitted under the EU-U.S. Data Privacy Framework Adequacy Decision and compare them to the legal standards allowed under EU law.

In accordance with the recital 141 of the EU-U.S. Data Privacy Framework Adequacy Decision the only legal source based on which bulk collection is performed is the E.O. 12333[291]. As emerges from the same recital, the only objective limitation to the bulk collection of personal data relates to the use of such personal data only for six defined objectives (which includes protecting 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). No additional criteria are specified, apart from assertions regarding the prioritization of targeted surveillance over bulk data collection and consideration of the impact that such bulk collection has "on the privacy and civil liberties of all persons"[292].

Firstly, E.O. 14086 does not influence existing legislation; it only impacts PPD-28. Additionally, the legitimate objectives outlined in this order, which justify intelligence activities, lack concise and clear formulation. They provide only generic wording, allowing for broad interpretation[293]. Additionally, there is no binding legislation that specifies the circumstances and conditions under which measures for bulk data processing may be adopted [294]. Additionally, there are no specifications regarding any legislative measures that would allow for the exceptional retention of data for a limited period, where such retention would be deemed necessary, appropriate, and proportionate within a democratic society for the six stated objectives[295]. Moreover, there is no specification regarding a review by a court or independent

[290] Schrems II judgment, para. 183.
[291] EU-U.S. Data Privacy Framework Adequacy Decision, recital 141.
[292] *Ibid.*
[293] Giacalone M., "Verso Schrems III ? Analisi del nuovo EU-US Data Privacy Framework", European Papers, Volume 8, No 1, 2023, pp. 149-157 available on https://doi.org/10.15166/2499-8249/644, p. 152 and 153.
[294] Read in light *Privacy International*, para. 68.
[295] Read in light of *Privacy International*, para. 58.

administrative body prior to granting access to the retained data by national authorities, nor is there clarification on the urgent situations in which this process could be circumvented[296]. Finally, there is no process requiring national authorities that have accessed data collected in bulk to notify affected individuals once there is no longer a risk to the outcome of the investigation. This absence of notification prevents those individuals from seeking legal redress if they believe their rights and freedoms have been infringed[297].

It is interesting the report provided by the Privacy and Civil Liberties Oversight Board on the Section 702 of the FISA, where it states that this section cannot be considered as authorising for bulk collection of data, but confirms that the program does not contain appropriate judicial review of targeting decisions (as only persons who lack recognised Fourth Amendment rights may be targeted under Section 702), which could lead to overbroad or unjustified targeting[298]. In the same report, the Privacy and Civil Liberties Oversight Board has pointed out that the target numbers and their associated selectors are continuously growing[299]. Within that context, the mentioned Board points out that the risk of too extensive collection of communications and its further use "is very real and can cause harm, at varying degrees, that the performed targeting presents a number of privacy risks and harms by authorizing surveillance of a large number of targets, providing only programmatic review of a surveillance program, allowing extensive incidental collection, and causing inadvertent collection, concluding that the FISC reviews and approves targeting procedures to minimize the risks of improper surveillance, but there is no individualized judicial review of targeting decisions"[300]. Regarding the incidental collection of data, the Board stated that there is currently no data on the magnitude of such collection affecting U.S. persons, and it did not mention the incidental collection of non-U.S. individuals[301]. The Board emphasised the critical importance of having at least estimated numbers to assess the associated risks; however, as the incidental collection of data is increasing, it can be concluded that the number of affected EU data subjects is also growing[302]. Additionally, as noted in the Report from 2013, the Section 702 of the FISA does not require

[296] Read in light of *Tele2 Sverige*, para. 120.
[297] Read in light of *Tele2 Sverige*, para. 121.
[298] Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, September 28, 2023, Privacy and Civil Liberties Oversight Board, p. 9, available on https://www.pclob.gov/Oversight.
[299] *Ibid*.
[300] *Ibid*.
[301] *Ibid*.
[302] *Ibid,* p. 10.

foreign intelligence information to be the sole or even primary purpose of acquisition; rather, it must be "a significant purpose of the acquisition"[303]. This means that there can be other purposes for data collection in addition to foreign intelligence. The declassified FISC opinions indicate that, as a result of the broad data collection implemented under the upstream programme, the collected personal data may not be relevant to foreign intelligence[304].

This extensive collection, which lacks individualised judicial review of targeting decisions—especially concerning the incidental collection of data affecting EU individuals whose data are transferred to the U.S.—exhibits the same deficiencies identified by the Court of Justice of the European Union in the *Digital Rights Ireland and Others* judgment. In that case, the Court found that individuals whose data were retained did not necessarily have any connection to situations that could give rise to criminal prosecutions[305]. Similarly as in the *Privacy International* case, the U.S. legislation does not provide rules to retain data for a limited period within the limits permitted in a democratic society[306]. Furthermore, U.S. legislation lacks mechanisms to ensure that affected individuals are notified about surveillance activities once there is no longer a risk of jeopardising ongoing investigations. This absence of notification hinders individuals' ability to seek legal redress if they believe their rights and freedoms have been infringed[307].

Although *stricto sensu* it cannot be considered to be considered as bulk collection of personal data, the report issued by the Privacy and Civil Liberties Oversight Board mentions a type of query known as "batch queries"[308]. Through these queries, FBI personnel can search information collected under Section 702 of the FISA using hundreds or thousands of query terms at once, allowing for the rapid processing of data[309]. These batch queries are not specified in the EU-U.S. Data Privacy Framework Adequacy Decision, but they could be considered to be a sort of bulk data processing as many different queries are simultaneously processed within a huge base containing information collected via Section 702 of the FISA. These a significant

[303] Report from 2013, p. 5.
[304] *Ibid.*
[305] *Digital Rights Ireland and Others*, paras. 58 and 69.
[306] *Privacy International*, para 58.
[307] In line with *Tele2 Sverige*, para. 121.
[308] Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, September 28, 2023, Privacy and Civil Liberties Oversight Board, p. 8, available on https://www.pclob.gov/Oversight.
[309] *Ibid*.

concern is that, as stated by the mentioned Board, these practices are performed "by allowing a single broad justification for hundreds or thousands of query terms" and they are not based on specific and individualised assessments for each discriminant which makes impossible to "ensure that the query standard is actually being met and only searches reasonably believed to return evidence of a crime or foreign intelligence are performed"[310].

Therefore, with regard to the bulk collection and further processing of personal data within the EU-U.S. Data Privacy Framework Adequacy Decision, and in line with the standards established by the Court of Justice of the European Union in *Digital Rights Ireland and Others*, *Tele2 Sverige* and *Privacy International* cases, we could not identify objectively defined criteria for interferences with fundamental rights as outlined in Articles 7 and 8 of the Charter. Furthermore, we have found that these interferences do not adhere to the proportionality requirement imposed by Article 52 of the Charter, nor have we identified any protective mechanisms available to individuals for these interferences, as defined in the aforementioned case law, and thus we cannot state that the mentioned Adequacy Decision has a "level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union"[311].

b. Oversight mechanisms under the EU-U.S. Data Privacy Adequacy Decision

The existence of an oversight mechanism is a crucial condition that must be met when the European Commission determines that a third country or international organisation provides an adequate level of protection, as stipulated in Article 45(2)(b) of the General Data Protection Regulation[312]. This condition has not been assessed by the Court of Justice of the European Union in cases related to previous data transfer mechanisms that were recognised as providing an adequate level of protection. Instead, the Court of Justice of the European Union focused solely on the redress possibilities available to individuals whose data were transferred, which are inherently linked to the oversight powers of an independent authority.

The implementation of a mechanism designed to oversee the protection of personal data is a requirement explicitly imposed by Article 8(3) of the Charter, which specifies that compliance

[310] *Ibid*, p. 17.
[311] Following a requirement articulated by the Court of Justice of the European Union in paragraph 73 of the Schrems I judgment.
[312] Article 45(2)(b) of the General Data Protection Regulation.

with data protection rules shall be subject to control by an independent authority[313]. Although this provision does not explicitly mention that such a requirement is necessary for third countries or international organisations to adopt an adequacy decision enabling data transfers to these entities, it can be inferred that any third country or international organisation providing adequate level of protection must also demonstrate the existence of an independent authority empowered to oversee compliance with data protection rules[314]. This requirement is clarified by the General Data Protection Regulation, which in its Article 45(2)(b), states that a third country or international organisation must provide an independent oversight mechanism to issue an adequacy decision. This provision stipulates the existence and effective functioning of one or more independent supervisory authorities, which must be responsible for ensuring and enforcing compliance with data protection rules. These authorities should possess adequate enforcement powers, assist and advise data subjects in exercising their rights, and cooperate with the supervisory authorities of the Member States[315].

In relation to the oversight described in Article 45(2)(b) of the General Data Protection Regulation, point (a) of the same paragraph states, among other elements, the necessity for a third country or international organisation to ensure effective and enforceable data subject rights, as well as effective administrative and judicial redress for data subjects whose personal data are being transferred[316]. Although both aspects are related, the oversight authorities must, as part of their role, assist and advise data subjects in exercising their rights, one of which is the ability to seek administrative and judicial redress. However, such redress constitutes a separate element to be assessed in the process of determining whether a third country or international organisation provides an adequate level of protection.

The EU-U.S. Data Privacy Framework Adequacy Decision relies on several oversight mechanisms.

As defined in title 2.3. *Administration, oversight and enforcement* of the currently valid adequacy decision, it is stated that the Department of Commerce, the Federal Trade Commission, and the Department of Transportation in the U.S. will carry out oversight and monitoring to verify and ensure compliance of organisations certified under the scheme agreed between the EU and the U.S[317]. However, these oversight roles relate only to activities

[313] Article 8(3) of the Charter.
[314] Article 45(2)(b) of the General Data Protection Regulation.
[315] *Ibid.*
[316] Article 45(2)(a) of the General Data Protection Regulation.
[317] Title 2.3. of the EU-U.S. Data Privacy Framework Adequacy Decision.

performed by self-certified organisations that have imported data from the EU and do not extend to overseeing activities involving transferred personal data when conducted for national security purposes. These activities, carried out by national security authorities, are subject to a complex monitoring system, as described in title 3.2.2. *Oversight* of the EU-U.S. Data Privacy Framework Adequacy Decision[318].

The first roles mentioned in the EU-U.S. Data Privacy Framework Adequacy Decision, responsible for overseeing compliance with applicable personal data protection rules, relate to the Inspector General, a Privacy and Civil Liberties Officer, and an officer or officers in a designated compliance role[319]. That provision is based on an obligation stipulated in the E.O. 14086 which requires each element of the Intelligence Community that collects signals intelligence to designate senior-level legal, oversight, and compliance officials to conduct periodic oversight of signals intelligence activities[320]. If such officials identify a significant incident of non-compliance with applicable U.S. laws, the situation must be promptly reported to the head of the respective body, the head of the relevant agency or executive department, and the Director of National Intelligence. Following such notification, the aforementioned heads and the Director of National Intelligence are required to take measures to remediate the incident and prevent its recurrence[321]. The difference between the status of supervisory authorities, which are independent bodies, and individual officers or departments within larger entities—such as inspector generals, privacy and civil liberties officers, and officers in designated compliance roles—is clear. However, we consider it prudent and appropriate to assess the function of these officers, given that the data protection system in a third country does not need to follow an identical approach to that of the EU, but must provide an essentially equivalent level of protection[322].

Therefore, the roles of the officers in question need to be assessed to determine whether they meet the requirement that independent supervisory authorities should be responsible for ensuring and enforcing compliance with data protection rules. This includes having adequate enforcement powers, assisting and advising data subjects in exercising their rights, and cooperating with the supervisory authorities of the EU Member States, as defined in Article 45(2)(b) of the General Data Protection Regulation.

[318] Title 3.2.2. of the EU-U.S. Data Privacy Framework Adequacy Decision
[319] EU-U.S. Data Privacy Framework Adequacy Decision, recital 163.
[320] Section 2(d)(i)(A) E.O. 14086
[321] Section 2(d)(iii) E.O. 14086
[322] Schrems I judgment, para. 73.

Firstly, the question to be answered is whether these roles can be considered "independent". Regarding the notion of the independence of supervisory authorities, in the case of *European Commission v. Republic of Austria*, the Court of Justice of the European Union found that the Austrian Federal Chancellery provided the Austrian supervisory authority with staff members who were required to independently oversee the proper implementation of data protection rules. However, as these staff members were simultaneously subject to supervision by the Chancellery, the Court concluded that this undermined the requirement of independence[323]. In a similar case, the issue was a premature termination of the term of office of the supervisory authority, and the Court of Justice of the European Union remarked the obligation to allow that authority to serve its full term of office[324]. Considering that the Inspector General, Privacy and Civil Liberties Officer, and officer or officers in a designated compliance role are staff members of the entities whose activities they need to supervise, it cannot be stated that they are "independent" as determined by the Court of Justice of the European Union in the case of *European Commission v. Republic of Austria*. Their term of office is not specifically protected, unlike the protected terms of the judiciary, and therefore the requirements defined by the Court of Justice of the European Union in the case of *European Commission v. Hungary* are also not met.

Secondly, these roles must be capable of "ensuring and enforcing compliance with data protection rules, including having adequate enforcement powers, assisting and advising data subjects in exercising their rights, and cooperating with the supervisory authorities of the Member States"[325]. One of the roles of the heads and the Director of National Intelligence is to take measures to remediate and prevent the recurrence of significant incidents of non-compliance[326], which demonstrates that the response to infringements of data protection rules is not driven independently but by the same entities that have infringed the rules. This clearly differs from Article 45(2)(b) of the General Data Protection Regulation. The redress mechanism provides a different approach, with the Director of National Intelligence responsible for designing a process that authorises the Civil Liberties Protection Officer of the Office of the Director of National Intelligence to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints[327]. After the finalisation of the investigation, when

[323] C-614/10, *European Commission v. Republic of Austria*, judgment of 16 October 2012, ECLI:EU:C:2012:631, paras. 59 and 63.
[324] C-288/12, *European Commission v. Hungary*, judgment of 8 April 2014, ECLI:EU:C:2014:237, para. 60.
[325] Article 45(2)(b) of the General Data Protection Regulation.
[326] Section 2(d)(iii) E.O. 14086
[327] Section 3(c)(i) E.O. 14086

communicating with data subjects, the Civil Liberties Protection Officer of the Office of the Director of National Intelligence informs the complainant, through the appropriate public authority in a qualifying state (with EU Member States considered qualifying states), without confirming or denying that the complainant was subject to U.S. signals intelligence activities. The response provided to data subjects states: "The review either did not identify any covered violations, or the [Civil Liberties Protection Officer of the Office of the Director of National Intelligence] issued a determination requiring appropriate remediation"[328]. Therefore, even in cases where the aforementioned officer is entitled to handle complaints, the data subject will not receive information on whether he or she was subject to U.S. signals intelligence activities, nor will they receive any substantial assistance or advice on exercising their rights.

Thus, in the context of national security activities, these officers, including the Civil Liberties Protection Officer of the Office of the Director of National Intelligence, have restrictions when performing their duties to ensure and enforce compliance with data protection rules and are not able to properly assist and advise data subjects in exercising their rights, as required by Article 45(2)(b) of the General Data Protection Regulation.

Besides national security activities, privacy and civil liberties officers, as well as inspectors general, are also designated within law enforcement bodies[329]. Their powers vary depending on the authorising statute and encompass the supervision of procedures to implement privacy and civil liberties concerns and to address complaints from data subjects[330]. Regarding the powers of the inspectors general, they can only issue non-binding recommendations[331]. Based on the context provided in the adequacy decision in question, there is no indication that within law enforcement bodies, the role of the privacy and civil liberties officers and inspectors general is essentially equivalent to that of the independent supervisory authorities described in Article 45(2)(b) of the General Data Protection Regulation.

It is important to note that in the adequacy decision in question, the Civil Liberties Protection Officer of the Director of National Intelligence (also known by the abbreviation ODNI CLPO) should not be confused with the privacy and civil liberties officers engaged within different national security or law enforcement bodies. The Civil Liberties Protection Officer of the Director of National Intelligence can only be dismissed by the Director of National Intelligence

[328] EU-U.S. Data Privacy Framework Adequacy Decision, recital 183.
[329] *Ibid*, recitals 108 and 109.
[330] *Ibid.*
[331] *Ibid.*

for cause, i.e., in cases of misconduct, malfeasance, breach of security, neglect of duty, or incapacity, thereby enjoying a level of protection that is not specifically mentioned in the adequacy decision for the role performed by the privacy and civil liberties officers[332].

The next oversight mechanism for national security activities listed in the EU-U.S. Data Privacy Framework Adequacy Decision is the Intelligence Oversight Board, which is established within the President's Intelligence Advisory Board and serves as an advisory body within the Executive Office of the President[333]. Article 45(2)(b) of the General Data Protection Regulation requires that the European Commission assess the existence and effectiveness of an independent supervisory authority that has responsibility for "ensuring and enforcing compliance with data protection rules, including adequate enforcement powers"[334]. As clearly emerges from the recital cited above of the adequacy decision in question, the aforementioned board has only advisory functions, along with various reporting functions, including reporting to the President, but does not have any enforcement functions nor a role in advising data subjects. Thus, the Intelligence Oversight Board is certainly not an independent supervisory authority with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, assisting and advising data subjects in exercising their rights, and cooperating with the supervisory authorities of the Member States. This is a crucial element to analyse when assessing the adequacy of the level of protection as required by Article 45(2)(b) of the General Data Protection Regulation.

Another oversight mechanism described in the EU-U.S. Data Privacy Framework Adequacy Decision is the Privacy and Civil Liberties Oversight Board, which has an oversight role in the law enforcement and national security spheres[335]. As previously mentioned, the Privacy and Civil Liberties Oversight Board is an independent agency within the executive branch, composed of five bipartisan members appointed by the President for a fixed six-year term, with Senate approval[336]. This Board involves two different powers in its election process: the executive and legislative branches[337]. Its fixed term of office protects the independence of its members from inappropriate external influence[338]. However, the fact that it is a bipartisan body could be an impediment to its independence as a supervisory authority, considering that Article

[332] EU-U.S. Data Privacy Framework Adequacy Decision, recital 179.
[333] *Ibid*, recital 166.
[334] Article 45(2)(b) of the General Data Protection Regulation.
[335] *Ibid*, recitals 110 and 167.
[336] *Ibid.*
[337] *Ibid.*
[338] *Ibid.*

52(2) of the General Data Protection Regulation states that members must remain free from external influence, whether direct or indirect. Party membership or political engagement could undermine such independence.

Regarding the powers of the Privacy and Civil Liberties Oversight Board, the key element to be assessed is whether it has the authority to ensure and enforce compliance with data protection rules, including adequate enforcement powers. The Board has the authority to review and analyse executive branch actions (regulations, policies, procedures, and data-sharing practices) to ensure a balance with the need to protect privacy and civil liberties[339]. It is also responsible for ensuring that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to the fight against terrorism[340]. The role of the Board was extended to additional tasks in accordance with E.O. 14086. Under this executive order, the Board is "encouraged" to review various policies and procedures related to intelligence activities, as well as the redress process[341]. The recipients of such reviews are required to "carefully consider and shall implement or otherwise address all recommendations contained in such report, consistent with applicable law"[342]. Upon performing the reviews, the Board produces various reports. However, none of these oversight activities are connected to any enforcement powers. Therefore, the element of ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, which must be considered when assessing the adequacy of the level of protection required by Article 45(2)(b) of the General Data Protection Regulation, does not exist. Thus, it can be concluded that this Board does not meet the adequacy level standard required by the cited provision.

The committees in the U.S. Congress (the House and Senate Intelligence and Judiciary Committees) have also been listed as oversight mechanisms by the European Commission in the EU-U.S. Data Privacy Framework Adequacy Decision. Although it is apparent at first glance that the committees of the U.S. Congress are not "independent authorities" in the sense of Article 8(3) of the Charter, nor "independent supervisory authorities" in a third country or international organisation, with responsibility for "ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, assisting and advising data subjects in exercising their rights, and cooperating with the supervisory authorities of the Member

[339] *Ibid.*
[340] 42 U.S.C. § 2000ee.
[341] Section 2 (v)(B), Section 3 (e) and Section 3 (e) of the E.O. 14086.
[342] *Ibid.*

States" as defined in Article 45(2)(b) of the General Data Protection Regulation[343], it is appropriate to provide straightforward reasoning in this regard.

The independence requirement is evident in the obligation of the supervisory authorities of the EU Member States to remain free from external influence, whether direct or indirect. They shall neither seek nor take instructions from anyone and must refrain from any action incompatible with their duties. During their term of office, they shall not engage in any incompatible occupation, whether gainful or not, and must have staffing and budgetary autonomy344. The specialised committees within the U.S. Congress are confirmed by members of political parties, raising questions about their ability to remain free from any direct or indirect external influence, including the influence of the bodies of the parties to which they belong. These committees are composed of legislators (senators and representatives) who primarily represent their electorate and are not selected or appointed to ensure and enforce compliance with data protection rules as supervisory authorities. Nothing in the EU-U.S. Data Privacy Framework Adequacy Decision indicates that these committees could ensure or enforce compliance with data protection rules, such as having the power to impose financial sanctions or to request that certain data be deleted or accessed by individuals. As stated in recital 169 of the currently valid adequacy decision, the President ensures that illegal intelligence activities are reported to the intelligence committees along with corrective actions[345], but such corrective actions are not to be taken by the committees in question. Therefore, the role of the committees is limited to the political and legislative sphere, without covering the obligation to address data subject complaints, take investigative actions, or provide advice and assistance in that regard, nor to cooperate with data protection supervisory authorities of the EU Member States.

Thus, it can be concluded that the committees of the U.S. Congress, which the European Commission stated have a role in overseeing the EU-U.S. Data Privacy Framework Adequacy Decision, are neither independent nor supervisory authorities. They also cannot ensure or enforce data protection rules, nor do they possess enforcement powers. Additionally, these committees have no role in assisting or advising data subjects in exercising their rights. Finally, regarding cooperation with the supervisory authorities of the EU Member States, such cooperation does not exist nor is it expected. Hence, the committees of the U.S. Congress

[343] Article 45(2)(b) of the General Data Protection Regulation.
[344] Article 52 of the General Data Protection Regulation.
[345] EU-U.S. Data Privacy Framework Adequacy Decision, recital 169.

described in the EU-U.S. Data Privacy Framework Adequacy Decision cannot be considered an oversight body in the sense of Article 45(2)(b) of the General Data Protection Regulation.

The last oversight mechanism mentioned by the European Commission in the EU-U.S. Data Privacy Framework Adequacy Decision is the FISC. The FISC is a tribunal comprised of judges appointed by the Chief Justice of the U.S. from among sitting U.S. district court judges, who have previously been appointed by the President and confirmed by the Senate[346]. The judges, who hold their positions for life tenure and can only be removed for good cause, serve on the FISC for staggered seven-year terms. FISA requires that the judges be drawn from at least seven different U.S. judicial circuits[347]. From this perspective, it is clear that the FISC is an independent body whose members, who are judges, enjoy the independence that characterises such a role.

However, the question is whether such a tribunal can be considered a supervisory authority. Article 45(2)(b) of the General Data Protection Regulation states that the elements to be assessed include the responsibility of such authorities for "ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, assisting and advising data subjects in exercising their rights, and cooperating with the supervisory authorities of the Member States"[348]. In accordance with the EU-U.S. Data Privacy Framework Adequacy Decision, the oversight role of the FISC involves receiving reports from the Department of Justice and the Office of the Director of National Intelligence on violations of Section 702 of the FISA related to targeting, minimisation, and querying procedures in accordance with Rule 13 of the FISC Rules of Procedure[349]. In addition, the Department of Justice and the Office of the Director of National Intelligence provide reports to the FISC twice per year, containing statistics on topics such as incidents and targeting trends. Regarding the mentioned Rule 13, it defines the obligation of the government to report if a submission to that court contained a misstatement or omission of material fact, and to report if an authority or approval granted by this court has been implemented in a manner that did not comply with the Court's authorisation or approval, or with applicable law[350].

[346] *Ibid*, recital 143 and footnote 260.
[347] *Ibid*.
[348] Article 45(2)(b) of the General Data Protection Regulation.
[349] EU-U.S. Data Privacy Framework Adequacy Decision, recital 173.
[350] Rule 13(b) of the Rules of Procedure of the United States Intelligence Surveillance Court, available at https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

However, as already mentioned in this work, the main role of the FISC is to review applications submitted by the Attorney General and the Director of National Intelligence based on Section 702 of FISA and to issue, if the conditions are met, annual certifications for surveillance[351]. These certifications relate to surveillance programmes rather than targeted surveillance activities, ensuring that individuals are properly targeted to acquire foreign intelligence information[352]. Considering the context provided by the European Commission in the EU-U.S. Data Privacy Framework Adequacy Decision, it could be reasonably stated that the role of the FISC is that of a tribunal which assesses whether surveillance requests received from law enforcement or national security bodies adhere to the applicable legal requirements and authorises them if they do.

Regarding the first element mentioned in Article 45(2)(b) of the General Data Protection Regulation, there is no reason to doubt that the FISC adopts decisions concerning the authorisation of surveillance activities in compliance with data protection rules. However, once a decision is adopted—meaning once the annual certification of a surveillance programme has been issued or the installation of pen registers or trap and trace devices has been approved—the role of the FISC is over, unless it is notified under the aforementioned Rule 13 of its Rules of Procedure about a misstatement, omission, or non-compliance. In such cases, the FISC can request remedial actions[353]. Another aspect to take into account is that there is no indication that the FISC would have the power to initiate, *suo motu*, oversight of the surveillance activities it has authorised. The power to initiate investigations into the implementation of data protection rules is an important element regarding the independence of supervisory authorities; that is, the power to schedule and determine their own oversight activities without being triggered by external parties, as is the case with the aforementioned Rule 13. Article 45(2)(b) of the General Data Protection Regulation also emphasises the role of supervisory authorities in "assisting and advising data subjects in exercising their rights"[354]. The FISC has no legal obligation to assist and advise data subjects in exercising their rights. This is another indicator that the FISC should be considered a tribunal whose role is to assess whether surveillance requests received from law enforcement or national security bodies are justified.

[351] Rodriguez S., „The United States of Surveillance: A Review of America's Mass Surveillance Laws, Programs, and Oversight", DHSI Conference & Colloquium, Volume 3, Iss. 2, 2021, https://doi.org/10.21428/f1f23564.f20c77b2.
[352] Schrems II judgemet, para. 179.
[353] EU-U.S. Data Privacy Framework Adequacy Decision, recital 174.
[354] Article 45(2)(b) of the General Data Protection Regulation.

Moreover, there are no provisions regarding any cooperation framework between the FISC and the supervisory authorities of the EU Member States, nor is there any evidence that such cooperation has ever existed. Thus, there is no evidence that this condition, as defined in Article 45(2)(b) of the General Data Protection Regulation, has ever been met, nor that there have been any contacts between the FISC and the aforementioned authorities.

Based on the outlined framework regulating the activities and role of the FISC, it can be reasonably concluded that the FISC functions as a tribunal that assesses whether surveillance requests received from law enforcement or national security bodies adhere to the applicable legal requirements and authorises them if they do. The FISC has the possibility to adopt remedial measures in certain situations if notified about a misstatement, omission, or non-compliance. However, aside from such remedial measures in specific circumstances, the role of the FISC cannot be compared to that of independent supervisory authorities as conceived under the General Data Protection Regulation.

In conclusion, regarding the oversight elements for law enforcement and national security activities provided in the EU-U.S. Data Privacy Framework Adequacy Decision, which should consist, as described in Article 45(2)(b) of the General Data Protection Regulation, of the "effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States", there fs no evidence that any of the listed oversight mechanisms relate to an authority that would meet the standards required by the mentioned provision[355]. Additionally, from the perspective of data subjects whose personal data have been transferred from the EU to the US, they cannot rely on the assistance and advice of any independent supervisory authority. Finally, the supervisory authorities of EU Member States do not have any of the mentioned bodies as counterparts with which to cooperate; although, under the redress mechanism, which will be further analysed, a specific type of cooperation in submitting and delivering requests and responses is provided.

[355] Article 45(2)(b) of the General Data Protection Regulation.

c. Redress mechanisms under the EU-U.S. Data Privacy Adequacy Decision

The redress deficiencies were evident from the outset in the first mechanism that granted self-certified U.S. organisations the status of providing an adequate level of protection. In the Schrems I judgment, the Court of Justice of the European Union found that the Safe Harbour Adequacy Decision lacked any finding on the existence of effective legal protection against interference by state bodies when pursuing legitimate objectives, such as national security. The procedures before the Federal Trade Commission were limited to commercial disputes, and the private dispute resolution mechanisms only concerned compliance by organisations importing data from the EU applying the Safe Harbor Principles. These mechanisms could not be applied to disputes relating to the legality of interference with fundamental rights resulting from measures originating from state bodies[356]. Therefore, it is evident that, as early as 2015, the Court of Justice of the European Union highlighted the importance of an effective mechanism for administrative and judicial redress for data subjects whose data is transferred from the EU to the U.S. under the relevant adequacy decision[357].

In the *Schrems II* judgment, which invalidated the Privacy Shield Adequacy Decision, the Court of Justice of the European Union identified severe discrepancies between the expected redress standards and those provided by that adequacy decision[358]. The Court found that while there were various redress mechanisms covering unlawful (electronic) surveillance for national security purposes, certain legal bases available to U.S. intelligence authorities, such as E.O. 12333, were not covered[359]. Additionally, the Court noted that even where judicial redress was possible, individuals' requests could easily be declared inadmissible if they could not demonstrate "standing", thereby limiting access to judicial protection, and finally concluded that it "does not confer rights which are enforceable against the U.S. authorities in the courts"[360]. Furthermore, in the Schrems II judgment, the Court of Justice of the European Union raises concerns about the role of the FISC, reiterating that its powers do not extend to ensuring the proper targeting of individuals when collecting foreign intelligence[361]. The Court of Justice of the European Union concludes that Section 702 of the FISA "does not indicate any limitations

[356] Schrems I judgment, paras. 88 and 89.
[357] *Ibid,* para 95.
[358] Schrems II judgment, paras. 196 and 197.
[359] *Ibid,* para. 191.
[360] *Ibid*, paras. 115 and 182.
[361] *Ibid.* 179.

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"[362]. In relation to Section 702 of the FISA, the Court of Justice of the European Union noted its finding that PPD-28, which was fully in force at the time, did not grant data subjects actionable rights before the courts against U.S. authorities[363]. This finding was contrary to the requirement in Article 45(2)(a) of the General Data Protection Regulation, which stipulates that one element of an equivalent level of protection is the empowerment of data subjects whose personal data are transferred, providing them with "effective and enforceable data subject rights"[364].

In that context, following two consecutive invalidations based, among other elements, on the lack of effective administrative and judicial redress for data subjects whose personal data are being transferred, the European Commission, in its communication regarding the adoption of the EU-U.S. Data Privacy Framework Adequacy Decision, stated that EU individuals will have access to an independent and impartial redress mechanism concerning the collection and use of their data by U.S. intelligence agencies[365]. This mechanism includes the newly created Data Protection Review Court.

Now we will proceed to analyse whether the redress mechanisms provided in the currently applicable adequacy decision for personal data transfers to the U.S. meet the standards defined in Article 45(2)(a) of the General Data Protection Regulation. This provision states that, when assessing the adequacy of the level of protection in a third country or international organisation, there should be an "effective administrative and judicial redress for the data subjects whose personal data are being transferred"[366]. As with the oversight mechanisms, it is also important to differentiate between the redress mechanisms concerning claims against self-certified organisations that imported personal data from the EU and those concerning access to transferred personal data by public authorities.

That said, the EU-U.S. Data Privacy Framework Adequacy Decision provides clear guidance on the available redress avenues concerning claims against self-certified organisations that

[362] *Ibid*, para. 180.
[363] *Ibid*, para. 181.
[364] 45(2)(a) of the General Data Protection Regulation.
[365] Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-U.S. data flows, Press Release of 10 July 2023, Brussels, available on https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.
[366] Article 45(2)(a) of the General Data Protection Regulation.

imported personal data from the EU. As mentioned previously, the current adequacy decision specifies that individuals can bring a complaint directly to an organisation, to an independent dispute resolution body designated by the organisation, to an EU data protection supervisory authority, to the Department of Commerce, or to the Federal Trade Commission[367]. If their complaints remain unresolved by any of these mechanisms, data subjects also have the right to invoke binding arbitration (Annex I of Annex I to the EU-U.S. Data Privacy Framework Adequacy Decision)[368]. Besides arbitration, judicial redress is also available under U.S. law, including the right to obtain compensation for damages[369]. Among the presented avenues, the option to engage an independent arbitration body is notable, as this possibility already existed in previous adequacy decisions. Additionally, the role of the EU data protection supervisory authorities is significant, as data subjects can lodge complaints with these authorities even in cases where they have not been designated as the organisation's dispute resolution body[370]. The available redress mechanisms concerning claims against self-certified organisations do not indicate any non-compliance with the requirement for administrative and judicial redress for data subjects whose personal data are being transferred.

On the other hand, the redress avenues available to data subjects when their transferred personal data is processed by U.S. public authorities for national security purposes have certain limitations that we will now assess.

The EU-U.S. Data Privacy Framework Adequacy Decision first highlights the role of the newly established Civil Liberties Protection Officer of the Director of National Intelligence as an administrative redress function established by E.O. 14086[371]. The redress process is initiated by a data subject who believes their rights have been violated in the context of the aforementioned adequacy decision. They submit their complaint to the EU Member State data protection supervisory authority responsible for public authorities, which will forward the claim to the European Data Protection Board, which will then send it to the U.S. authorities[372]. The complaint must contain basic information, such as the personal data reasonably believed to have been transferred to the U.S. and the means by which it is believed to have been transferred[373].

[367] EU-U.S. Data Privacy Framework Adequacy Decision, recital 68.
[368] *Ibid*.
[369] *Ibid*, recital 86.
[370] *Ibid*, recitals 73 and 77.
[371] Section 3 (c)(i) of the E.O. 14086.
[372] EU-U.S. Data Privacy Framework Adequacy Decision, recital 177.
[373] *Ibid*, recital 178.

Once received by the U.S. authorities, the initial investigation will be conducted by the Civil Liberties Protection Officer of the Director of National Intelligence, who is authorised to access all information processed by the national security authorities and to assess whether the activities performed were in line with U.S. law[374]. Upon completing the review of the complaint, the Civil Liberties Protection Officer of the Director of National Intelligence responds to the complainant through the EU Member State authority that channelled the complaint with the following: "the review either did not identify any covered violations or the ODNI CLPO issued a determination requiring appropriate remediation"[375].

Additionally, data subjects, as well as each affected element of the U.S. intelligence services, may seek a review of the decision made by the Civil Liberties Protection Officer of the Director of National Intelligence before the Data Protection Review Court[376]. The Data Protection Review Court is an independent tribunal established by the Attorney General under E.O. 14086 and consists of at least six judges appointed for renewable terms of four years[377]. Before the Data Protection Review Court, the interests of the concerned data subject are represented by a special advocate who can seek information from the data subject through written questions[378]. In cases where the process before the Data Protection Review Court was triggered by an application from the data subject, he or she will be notified through the relevant EU Member State authority that the review by the court has been completed and that "the review either did not identify any covered violations or the DPRC issued a determination requiring appropriate remediation"[379].

It is now appropriate to analyse whether the redress mechanisms meet the standards required by EU law, specifically whether the administrative and judicial redress offered is, in fact, effective, as required by Article 45(2)(a) of the General Data Protection Regulation. In line with that, it is important to point out the views of the Court of Justice of the European Union in Schrems II judgment, where it stated that "such effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since, as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and

[374] *Ibid*, recitals 179 and 180.
[375] *Ibid*, recital 183.
[376] *Ibid*, recitals 183 and 184.
[377] *Ibid*, recital 185.
[378] *Ibid*, recitals 183 and 188.
[379] *Ibid*, recital 192.

means to take effective action in relation to data subjects' complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country"[380].

The redress mechanisms established under the invalidated Privacy Shield Adequacy Decision have been found to be insufficient. Therefore, in this work, we will analyse the redress mechanism introduced by the EU-U.S. Data Privacy Framework Adequacy Decision, specifically the Civil Liberties Protection Officer of the Director of National Intelligence before the Data Protection Review Court.

The administrative aspect of the redress mechanism established by E.O. 14086 is based on the role of the Civil Liberties Protection Officer of the Director of National Intelligence, who has the authority to review the necessary information and investigate complaints within their statutory and delegated authority, and who must not only consider "applicable privacy protections but also the relevant national security interests, along with giving appropriate deference to any relevant determinations made by national security officials" and implement the law impartially[381]. Within this context, special attention should be given to the fact that complaints must be resolved by considering the "applicable privacy protections" alongside with "the relevant national security interests".

A deeper analysis indicates that the term "applicable privacy protections" is not specifically defined within E.O. 14086; however, the wording unquestionably relates to applicable legal protections, in the sense of legal provisions from laws, executive orders, and other legal sources relevant to the specific case being addressed, which relate to "privacy", a term that in the U.S. encompasses personal data. Nevertheless, the "privacy protections" cannot be applied independently but must be assessed alongside "the relevant national security interests", meaning that in certain cases such interests could override the "applicable privacy protections". Regarding the notion of "relevant national security interests", the E.O. 14086 states that the collection of signals intelligence is carried out to ensure that U.S. national security decision-makers can advance national security interests, without further explanations of what may constitute a relevant national security interest[382]. However, not every national security interest is valid for balancing against the "applicable privacy protections", but only those that are relevant, thereby limiting the scope of the interests to be considered. Such relevant interests do

[380] Schrems II judgment, para. 189.
[381] Section 3 (c)(A) and (B) of the E.O. 14086.
[382] Section 1 of the E.O. 14086.

not necessarily have to be significant, meaning that even a minor interest may be deemed relevant in a given case. Yet, the most problematic term is certainly “interests”, as an interest is not defined by law, can change over time depending on various factors, and the E.O. 14086 does not provide any guidance on what constitutes a relevant interest that could limit the application of “privacy protections”. In this sense, the system implemented for addressing claims from data subjects ensures that a veil is maintained over the parameters considered by the Civil Liberties Protection Officer of the Director of National Intelligence. It is highly questionable whether such a system, where legal sources can be overridden by undefined and non-public interests, can ensure “effective and enforceable data subject rights” as required by Article 45(2)(a) of the General Data Protection Regulation.

However, the heart of the hidden practices in the redress mechanism relates to the undisclosed final administrative and judicial decisions and their complete lack of reasoning. Once the redress process carried out by the Civil Liberties Protection Officer of the Director of National Intelligence, or, in the case of an appeal, the Data Protection Review Court, is completed, the data subject who submitted the request receives a response stating that "the review either did not identify any covered violations or the [Civil Liberties Protection Officer of the Office of the Director of National Intelligence or the Data Protection Review Court (if applicable)] issued a determination requiring appropriate remediation"[383].

Firstly, the initial question that arises is not related to any legal concern but rather why someone would appeal a decision from an administrative body that has confirmed either that no violations were identified or that it has issued a determination for the remediation of identified violations, especially knowing that the response to the appeal is, in essence, the same as the one received in the first instance. Clearly, this approach undermines the trust of data subjects in the redress system, decreases their interest in initiating any redress process, and raises reasonable suspicions about the effectiveness and enforceability of data subject rights within the redress process.

Secondly, it is necessary to analyse the lack of reasoning in the final responses provided by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence and by the Data Protection Review Court. It is pertinent to determine whether the response from the Civil Liberties Protection Officer or the Data Protection Review Court constitutes a decision or is merely a template-based answer. The response does not indicate whether the data subject's

[383] Section 3 (c)(iii)(E)(1) and (d)(i)(H) of the E.O. 14086.

claim has been accepted or rejected, nor does it specify what actions have been taken by the competent U.S. authorities, without even addressing the necessity for reasoning. Thus, it cannot be concluded that any decision is communicated to the data subject; rather, the redress process is terminated with an ambiguous answer that, from the perspective of the data subject, is effectively meaningless.

Now, it is appropriate to assess whether the lack of any reasoned response resulting from the redress mechanism is in line with EU law.

Regarding the duty to provide a reasoning for administrative and judicial decisions, in the case *Commission and Others v Kadi*, the Court of Justice of the European Union stated that the courts of the EU must ensure fundamental rights that "include, inter alia, respect for the rights of the defence and the right to effective judicial protection, emphasising that the later one, which is affirmed in Article 47 of the Charter, requires that the person concerned must be able to ascertain the reasons upon which the decision taken in relation to him is based, either by reading the decision itself or by requesting and obtaining disclosure of those reasons"[384].

Laffranque states that Article 6 of the European Convention on Human Rights and Fundamental Freedoms and Article 47 of the Charter, as interpreted by the European Court of Human Rights and the Court of Justice of the European Union, encompass within the right to an effective remedy and a fair trial the duty to provide reasons. She also notes that this duty primarily pertains to decisions made by the institutions of the EU, as well as to the administrative decisions of EU Member States when implementing EU law[385]. The same author also states that the rich case law of the European Court of Human Rights imposes strict standards upon the Member States as regards the motivation of judgments and important administrative decisions, in both civil and criminal cases, being domestic bodies obliged to provide clear reasoning for their decisions, covering the essential matters of the case[386].

In line with Laffranque, Opdebeek and De Somer highlight that the legal basis for a general duty to give reasons is found in Article 41 of the Charter, which refers to the right to good administration. They indicate that it is the duty of the administration to provide reasons for its decisions, while the Charter confers a (fundamental) right on citizens derived from a duty or

[384] Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, *European Commission and Others v Yassin Abdullah Kadi*, judgment of 18 July 2013, ECLI:EU:C:2013:518, paras. 97, 98 and 100.
[385] Laffranque J., „(Just) Give Me A Reason...", Juridica International, Volume 27, University of Tartu, Tartu, 2018, p. 14, available on https://doi.org/10.12697/JI.2018.27.02.
[386] *Ibid*, p. 17-18.

obligation[387]. The same authors also state that, although the aforementioned Article of the Charter refers explicitly to EU institutions and bodies, the Court of Justice of the European Union considers the principle of good administration—and within it the duty to give reasons—as an unwritten general principle of law applicable when EU Member States implement EU law[388]. After comparing various administrative systems in the EU, Opdebeek and De Somer conclude that the duty to give reasons provides both preventive and ex post facto legal protection to individuals. As they say, when adopting decisions, administrative bodies must reflect on the "legality, quality, rationality, reasonableness and fairness of their decisions" which minimise the chances for flawed decisions, and simultaneously enabling individuals to challenge that reasoning before the courts[389].

The European Commission, in the currently valid adequacy decision for data transfers to U.S. self-certified organisations, states that the lack of reasoning "allows protection of the confidentiality of activities conducted to protect national security, while providing the individuals with a decision confirming that their complaint has been duly investigated and adjudicated"[390].

However, Articles 41 and 47 of the Charter do not specify any possibility of limitations on the rights defined within them, which include the duty to provide reasoning. Furthermore, as stipulated in Article 52 of the Charter, limitations on the exercise of the rights and freedoms recognised by the Charter "must be provided for by law and must respect the essence of those rights and freedoms"[391]. Nevertheless, the European Commission has not provided any details on the extreme limitation imposed regarding the avoidance of communicating a decision and the related lack of reasoning at the end of the redress process.

In addition, as noted in Laffranque's analysis, Article 6 of the European Convention on Human Rights and Fundamental Freedoms also encompasses the right to obtain reasoning for judicial and significant administrative decisions[392]. In relation to this Convention, Article 52(3) of the Charter specifies that if the Charter contains rights corresponding to those guaranteed by the

[387] Opdebeek I., i De Somer S., „The Duty to Give Reasons in the European Legal Area a Mechanism for Transparent and Accountable Administrative Decision-Making? A Comparison of Belgian, Dutch, French and EU Administrative Law", ROCZNIK ADMINISTRACJI PUBLICZNEJ 2016(2), Uniwersytet Jagielloński, Krakow, p. 101.
[388] *Ibid*, p. 102.
[389] *Ibid*, p. 106.
[390] EU-U.S. Data Privacy Framework Adequacy Decision, recital 183.
[391] Article 52(1) of the Charter.
[392] Convention for the Protection of Human Rights and Fundamental Freedoms, *Council of Europe*, 1950, available on: https://www.echr.coe.int/documents/convention_eng.pdf

Convention, the meaning and scope of those rights shall be the same as those laid down by the Convention, even allowing for EU law to provide more extensive protection[393]. However, concerning the duty to provide reasoned decisions, the EU-U.S. Data Privacy Framework Adequacy Decision accepts as adequate an administrative and judicial redress system that offers less protection than that provided by the Convention.

In conclusion, regarding the redress process that, upon termination, provides a template response without reasoning to the data subject, we contend that such a redress process cannot be deemed effective, as required by Article 45(2)(a) of the General Data Protection Regulation. Furthermore, it does not align with the EU standards defined in Articles 41 and 47 of the Charter, as interpreted by the Court of Justice of the European Union, nor with Article 6 of the European Convention on Human Rights and Fundamental Freedoms, as interpreted by the European Court of Human Rights.

As a final note, having analysed the bulk collection of personal data, the various oversight mechanisms, and the administrative and judicial redress mechanisms provided by the EU-U.S. Data Privacy Framework Adequacy Decision, we conclude that all these elements exhibit significant deficiencies that render the aforementioned decision vulnerable to invalidation by the Court of Justice of the European Union.

10. Recent federal legislative efforts in the U.S. and conditions to meet EU data protection level

a. The deficiencies of the American Privacy Rights Act

As previously mentioned, one of the defining characteristics of the data protection landscape in the U.S. is the vacuum created by the absence of a federal data protection law and the fragmentation of regulations. At the federal level, sector-specific data protection laws apply, while at the state level, data protection laws primarily focus on consumer rights related to the processing of personal data by businesses.
Currently in the U.S., a draft of a federal data protection law, called the American Privacy Rights Act (hereinafter: APRA), is under discussion[394]. As explained by the Congressional Research Service, APRA would establish a comprehensive federal consumer privacy

[393] Article 52(3) of the Charter.
[394] H.R.8818 - American Privacy Rights Act of 2024, available on https://www.congress.gov/bill/118th-congress/house-bill/8818/text.

framework by incorporating elements of the American Data Privacy and Protection Act[395]. The proposed APRA provides definitions and obligations comparable to those defined in the General Data Protection Regulation. However, the draft law includes a set of exceptions that significantly affect its applicability and the level of data protection enjoyed by EU data subjects.

Although Section 101 (12)(A) of the APRA specifies that the term 'covered data' refers to information that identifies or is linked, or is reasonably linkable, either alone or in combination with other information, to an individual or a device that identifies or is linked, or reasonably linkable, to one or more individuals, certain categories are exempt. These include employee-related information, publicly available information, inferences drawn solely from multiple independent sources of publicly available information (without sensitive covered data or combined with covered data), information in the collection of a library, archive or museum, and on-device data. These exceptions demonstrate that significant sets of personal data, and the processing activities performed on such data, are not protected by the rules defined in APRA, leaving individuals without any protection of their personal data when such activities occur. This exclusion from the scope of applicability does not align with EU standards and represents one of APRA's key obstacles to being considered as a legislative draft that ensures alignment of U.S. data protection standards with those of the EU.

APRA's applicability ratione personae also presents key inconsistencies with EU data protection standards. The proposed bill excludes small businesses, Federal, State, Tribal, territorial, or local government entities, as well as entities collecting, processing, retaining, or transferring covered data on behalf of these government bodies, from its scope. Specifically, when such entities act as service providers to government entities, they are exempt[396]. These exclusions remove a significant group of entities from the bill's scope, particularly public entities related to Federal and State governments, along with their service providers. This leads to the conclusion that, despite the obligations outlined in APRA, data subjects would not enjoy enforceable rights against these entities, thereby failing to meet the requirements of Article 45(1) and (2) of the General Data Protection Regulation. With regard to the exclusion of small businesses, the impact on data protection is not determined by the size of a business but by the nature of its processing activities. These exemptions, particularly those related to public authorities and entities processing personal data as service providers, pose a significant and

[395] The American Privacy Rights Act, Congressional Research Service (CRS), available on https://crsreports.congress.gov/product/pdf/LSB/LSB11161.
[396] Section 2, paragraph (10) (A) (iii) of the APRA.

fundamental obstacle to considering APRA as a legislative mechanism capable of addressing the deficiencies in the U.S. legal system regarding the processing of personal data transferred from the EU.

Given the limitations of the proposed APRA, we will now analyse the requirements that a third country's legal framework and practices must meet to be considered as providing an adequate level of protection, and explore how the U.S. could establish a stable mechanism for receiving data from the EU..

b. Conditions for safe and stable transfers of personal data from the EU to the U.S.

Although the conditions for meeting the required level of adequate protection are clear, it is challenging for third countries to satisfy them. This is evident from the short list of G20 countries that have been granted such status—Argentina, Canada, the Republic of Korea, Japan, and U.S. organisations under the Data Privacy Framework—while other countries, such as Australia, Brazil, India, Indonesia, Mexico, Saudi Arabia, South Africa, and Turkey, have not been recognised, despite having data protection legislation[397]. Additionally, based on the experience with frameworks used for transferring data to the U.S., it has become evident that maintaining an adequate level of protection is difficult, especially when data protection activists challenge these frameworks with strong arguments, despite the European Commission's interest in preserving them.

The characteristics of the U.S. system present further obstacles. Firstly, there is the territorial fragmentation of data protection laws, with some states adopting their own laws, mainly focused on consumer data protection. Secondly, the U.S. has sector-specific laws addressing the processing of personal data at the federal level. The most well-known federal data protection laws include the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act. Additionally, the U.S. Privacy Act governs the processing of personal data by federal agencies but includes a wide range of exceptions related to administrative and law enforcement purposes. Furthermore, it only protects U.S. citizens and permanent residents, thereby excluding the majority of data

[397] From this snapshot covering G20 and their adequacy level, we did not count the People's Republic of China and the Russian Federation considering their approach to data protection which is significantly opposed to the EU standards, nor the United Kingdom as their data protection system is based on the EU standards that that country helped to build until it left the EU, significantly helping it to acquire the adequate level of protection.

transferred from the EU to the U.S.[398] Given the existing gaps between the EU and U.S. data protection frameworks, some authors anticipate a potential regulatory confluence in the long term if the EU successfully leverages a greater regulatory influence over the U.S.[399]

From the EU perspective, as already exposed in this work, the General Data Protection Regulation provides a clear set of elements that must be analysed by the European Commission when assessing the adequacy of the level of protection. In point (a) of Article 45(2), the General Data Protection Regulation mentions the necessity to assess the rule of law, the respect for human rights and fundamental freedoms, along with the relevant legislation, law enforcement and national security practices, data subject rights, and effective administrative and judicial redress for the data subjects whose personal data are being transferred[400]. This provision goes beyond pure data protection standards and prioritises the notion of the rule of law and respect for human rights and fundamental freedoms. It shows that an effective data protection framework cannot coexist within a legal system that does not uphold these principles, making it unattainable for countries that do not comply with such values to be recognised as providers of an adequate level of protection.

In the next point, the General Data Protection Regulation requires a functioning and effective independent supervisory authority capable of enforcing data protection rules, assisting and advising the data subjects in exercising their rights, and cooperating with the supervisory authorities of the Member States[401]. This highlights that the mere existence of a legal framework is not enough; it must also be applied in practice to ensure that the processing of transferred personal data is overseen and enforced. Finally, point (c) of the mentioned paragraph requires an assessment of the international commitments that the concerned third country has entered into[402].

The most stable and permanent solution for data transfers to the U.S. would be a comprehensive data protection law that addresses all the requirements of the General Data Protection Regulation and adheres to the clarifications provided in guidelines issued by EU regulators. However, given the limitations of the U.S. data protection legal framework—such as the

[398] 5 U.S. Code § 552a - Records maintained on individuals.
[399] Gao X., and Chen X., "Understanding the Evolution of Transatlantic Data Privacy Regimes: Ideas, Interests, and Institutions", Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24), Association for Computing Machinery, New York, USA, 2024, available on https://doi.org/10.1145/3655693.3655720, pp. 55.
[400] Article 45(2)(a) of the General Data Protection Regulation.
[401] Article 45(2)(b) of the General Data Protection Regulation.
[402] Article 45(2)(c) of the General Data Protection Regulation.

segmentation of data protection rules, the focus on consumer data protection practices, and laws that primarily protect the rights of U.S. citizens and aliens with permanent residence—it is unlikely that the U.S. will adopt a law that significantly changes this approach to cover all types of personal data processing, regardless of the entities involved. On the other hand, a more feasible approach to implementing the required data protection standards might be an international agreement between the U.S. and the EU, similar to what was established with the "Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences"[403], based on which the U.S. extended judicial redress to EU data subjects through the adoption of the Judicial Redress Act[404]. This approach would need to be much more detailed and extensive than the aforementioned agreement and could provide a privileged level of protection to EU data subjects, aligned with EU standards, without requiring the U.S. to alter the protection afforded to other data collected outside the scope of the General Data Protection Regulation.

Regardless of the avenue chosen to implement appropriate data protection improvements, it is essential to recognise that, without substantial changes in the U.S. data protection approach—particularly concerning oversight and redress mechanisms—data subjects will lack confidence that their rights are respected. Similarly, businesses involved in data transfers will be uncertain about the legality of the mechanisms they are using to transfer personal data and whether they will need to seek out and implement alternative mechanisms to replace previous ones, as occurred with the invalidation of the Safe Harbour and Privacy Shield adequacy decisions. Therefore, it is crucial to focus on the essential improvements that the U.S. must undertake to ensure that its data protection standards are essentially equivalent to those in the EU. The backbone of data protection in the EU is defined by the General Data Protection Regulation, while the broader framework of human rights and fundamental freedoms is articulated in the EU Charter of Fundamental Rights.

The predecessor of the EDPB, the Article 29 Working Party, adopted the Adequacy Referential, which provides details about the key elements that a third country's legal framework must

[403] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (OJ 2016 L 336, p. 3).
[404] Judicial Redress Act of 2015, Public Law 114–126 — Feb. 24, 2016, available on https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.

possess to be recognised as a provider of an adequate level of protection[405]. In the Adequacy Referential, it is required that data protection concepts are compatible with those existing under EU legislation and that data processing adheres to the principles applied in the EU, namely the obligation to process personal data for clearly defined purposes, to collect only the necessary data, and to retain it for the minimum necessary period[406]. It is essential to ensure the confidentiality, integrity, and availability of data are protected, while regarding the collection and further processing of personal data, this should only occur if a specific legal basis is met, with more restrictive rules applying to sensitive data[407]. Finally, a third country providing an adequate level of protection must ensure that data subjects are properly informed about the processing of their personal data and have the rights to access, rectify, delete, and object to the processing[408]. Concerning onward transfers, once personal data is transferred from the EU to a third country with an adequate level of protection, such data should, in essence, be equally protected[409].

The main concern regarding these material requirements relates to the wide scope of indiscriminate bulk collection of personal data. This framework is broadly outlined in recital 141 of the EU-U.S. Data Privacy Framework Adequacy Decision, where only the purposes of processing are described. In this context, substantial improvements are needed to clarify that bulk collection should only occur exceptionally. There should also be clear concepts to identify the conditions that trigger such exceptional bulk collection (to prevent the exception from becoming a rule), definitions of the retention periods for data collected in bulk, specifications of the types of data subject to such bulk collection, and proper notification of the affected individuals about this collection, provided that this information can be safely communicated without jeopardising the purpose of processing.

In the context of procedural and enforcement mechanisms, crucial improvements are needed, as there are clear deficiencies in independent oversight[410]. The U.S. should establish one or more independent supervisory authorities tasked with monitoring the lawfulness of data processing activities carried out by public entities on transferred personal data, particularly

[405] Article 29 Working Party Adequacy Referential Adopted on 6 February 2018, as last revised and adopted on 28 November 2017, p. 5 and 6.
[406] *Ibid.*
[407] *Ibid.*
[408] *Ibid.*
[409] *Ibid.*
[410] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, p. 12.

regarding law enforcement and national security purposes. These authorities should have the right to conduct investigations on their own initiative, rather than only responding to reports received from other entities or data subjects.

Moreover, these entities must be independent, with their own staff and board members who serve for a protected term of office, which can only be terminated for strict and objective reasons. They should also have a sufficient budget to operate independently and possess the authority to investigate and enforce appropriate remedial measures to address identified infringements and prevent future ones. Additionally, these authorities should be able to advise and cooperate with data subjects, receive submissions from them, and inform them about their rights and the status of their submissions. Finally, such authorities in third countries with an adequate level of protection must be capable of cooperating with EU data protection authorities. The establishment of these independent oversight bodies in the U.S. has been a persistent deficiency in the two invalidated data transfer frameworks and in the current EU-U.S. Data Privacy Framework.

Along with an effective independent oversight authority, the U.S. legal framework needs to implement a robust redress system that ensures individuals whose data have been transferred from the EU to the U.S. can seek administrative and judicial remedies for any infringements they have suffered in relation to the processing of their personal data. It is evident that the administrative and judicial redress mechanisms available for processing by self-certified entities under the EU-U.S. Data Privacy Framework differ significantly from those available when individuals seek redress from public authorities. Therefore, when their data is processed by public authorities—especially when law enforcement and national security bodies obtain data from self-certified organisations under the current adequacy decision—data subjects should have the ability to access effective administrative redress, participate in procedures, and receive information about the activities carried out with their personal data. They should also know whether their data protection rights have been infringed and receive a reasoned decision regarding any such infringement. To achieve this requirement, a potential solution could be in line with the previously mentioned “Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences” which would require the U.S. to amend its legislation and enable EU data subjects to access U.S. courts.

11. Conclusion

The evolution of data transfer mechanisms between the EU and the U.S. underscores the complexities of harmonising personal data protection across jurisdictions with significantly different legal frameworks. This work has explored the historical trajectory of these mechanisms, the critical decisions of the Court of Justice of the European Union that invalidated both the Safe Harbour and Privacy Shield Adequacy Decisions, and the introduction of the new EU-U.S. Data Privacy Framework.

The concerns affecting data transfers from the EU to the U.S. were triggered by the discovery of the secret surveillance programmes of the U.S. intelligence community and complaints submitted by data protection activists. These led to the invalidation of the Safe Harbour Adequacy Decision by the Court of Justice of the European Union. The main reasons for the invalidation were the ability of U.S. authorities to access personal data transferred to the U.S. beyond what was necessary and proportionate for national security, and the lack of any redress mechanism available to EU data subjects regarding activities conducted by U.S. public authorities. Following the invalidation of the Safe Harbour Adequacy Decision, the EU adopted the Privacy Shield Adequacy Decision, which was also invalidated due to U.S. surveillance for foreign intelligence purposes without guarantees for non-U.S. persons, and the lack of an effective redress mechanism involving an independent tribunal.

We note that the data protection deficiencies are still persistent in the currently valid mechanism for transfers to the U.S., the EU-U.S. Data Privacy Framework Adequacy Decision, jeopardising its sustainability. The bulk collection of personal data without prior court authorisation for specific measures remains a flaw, considering the lack of judicial authorisation for bulk collection and the inexistent legislative measures providing for limited data retention necessary for national security or proper notification of affected EU data subjects. The oversight mechanisms described in the current adequacy decision do not include an independent supervisory authority with enforcement powers and the authority to initiate proceedings independently. EU data subjects cannot rely on these oversight bodies for substantial cooperation with EU Member State supervisory authorities. Lastly, the new redress mechanism for national security purposes is not effective as it limits data subjects' participation and does not provide a specific response to complaints.

These considerable flaws in the EU-U.S. Data Privacy Framework Adequacy Decision require improvements to ensure an enduring and trustworthy mechanism for data transfers based on an

adequacy decision from the EU to the U.S. The American Privacy Rights Act, currently under legislative discussion, does not fulfil these requirements. Major amendments to U.S. legislation are needed to address identified deficiencies, including changing the bulk data collection approach and implementing effective, independent, and cooperative oversight and redress mechanisms. These legislative improvements could follow the example of the agreement between the EU and the U.S. in the field of personal data protection with regard to crime prevention, investigation, detection, and prosecution.

This work shows that without these changes, EU data subjects cannot enjoy the same level of protection they have under EU legislation, and data exporters from the EU and importers from the U.S. will lack certainty about the durability of the transfer mechanism they rely on. However, achieving a common approach in jurisdictions with different data protection perspectives, like the EU and the U.S., is challenging despite significant economic connections. This is evidenced by the limited number of third countries recognised by the EU as providing adequate protection, and the U.S. has demonstrated it is not an exception. Therefore, given the lack of solid improvements in the U.S. approach towards protecting data transferred from the EU, the history of adequacy decision invalidations may repeat cyclically until it is understood that protecting personal data is a win-win solution not only for data subjects but also for all involved stakeholders.

References

1. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (OJ 2016 C 202, p. 1).
2. Charter of Fundamental Rights of the European Union (OJ 2016 C 202, p. 389).
3. Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Rome 1950, available on: https://www.echr.coe.int/documents/convention_eng.pdf.
4. Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (OJ 2016 L 336, p. 3).
5. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ 2011 L 55, p. 13).
6. 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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1).
7. 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, p. 31).
8. 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) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11).
9. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).
10. 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 U.S.

Department of Commerce (notified under document number C(2000) 2441)) (OJ 2000 L 215, p. 7).

11. Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).
12. 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) (OJ 2016 L 207, p. 1).
13. 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-U.S. Data Privacy Framework (OJ 2023 L 231, p. 118).
14. Adequacy Referential Adopted on 28 November 2017 as last Revised and Adopted on 6 February 2018, WP 254 rev.01, Article 29 Working Party, available on: https://ec.europa.eu/newsroom/article29/items/614108.
15. 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, version 2.0, adopted on 18 June 2021, available on: https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.
16. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures Adopted on 10 November 2020, European Data Protection Board, available on https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.
17. Judicial Redress Act of 2015, Public Law 114–126 — Feb. 24, 2016, available on https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.
18. 5 U.S. Code § 552a, available on https://uscode.house.gov/view.xhtml?req=Title+18&f=treesort&num=141.

19. 42 U.S.C. § 2000ee, available on https://uscode.house.gov/view.xhtml?req=(title:42%20section:2000ee-1%20edition:prelim).
20. Presidential Policy Directive -- Signals Intelligence Activities, Policy Directive/PPD-28 of January 17, 2014, available on: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities#_ftn5.
21. Executive Order 14086 of October 7, 2022 "Enhancing Safeguards for United States Signals Intelligence Activities", available on https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.

Communications, reports and press releases:

1. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM/2013/0847 final), available on https://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF
2. Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-U.S. Data Flows (COM(2013) 846 final), available on https://eur-lex.europa.eu/resource.html?uri=cellar:4d874331-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF
3. Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-U.S. data flows, Press Release of 10 July 2023, Brussels, available on https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721
4. Press Release of November 6, 2015, European Commission, available on https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_15_6015/IP_15_6015_EN.pdf
5. Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, 18.10.2017, COM(2017) 611 final, CELEX number: 52017SC0344.
6. Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield, 19.12.2018, COM(2018) 860 final, CELEX number: 52018SC0497.

7. Report from the Commission to the European Parliament and the Council, on the third annual review of the functioning of the EU-U.S. Privacy Shield, 23.10.2019, COM(2019) 495 final, CELEX number: 52019SC0390.
8. Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection of 27 November 2013, available on https://cdn.netzpolitik.org/wp-upload/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf
9. Report on the U.S. NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (Report - A7-0139/2014), available on https://www.europarl.europa.eu/doceo/document/A-7-2014-0139_EN.html
10. H.R.8818 - American Privacy Rights Act of 2024, available on https://www.congress.gov/bill/118th-congress/house-bill/8818/text
11. Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, September 28, 2023, Privacy and Civil Liberties Oversight Board, p. 9, available on https://www.pclob.gov/Oversight
12. Rules of Procedure of the United States Intelligence Surveillance Court, available on https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf
13. The EU-U.S. Data Privacy Framework: Background, Implementation, and Next Steps, 24 October 2022, Congressional Research Service, p. 2, available on https://crsreports.congress.gov/product/pdf/LSB/LSB10846.

Jurisprudence:

1. C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, judgment of 16 July 2020, ECLI:EU:C:2020:559.
2. C-293/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, judgment of 8 April 2014, ECLI:EU:C:2014:238.
3. Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, *European Commission and Others v Yassin Abdullah Kadi*, judgment of 18 July 2013, ECLI:EU:C:2013:518.
4. C-288/12, *European Commission v. Hungary*, judgment of 8 April 2014, ECLI:EU:C:2014:237.

5. C-614/10, *European Commission v. Republic of Austria*, judgment of 16 October 2012, ECLI:EU:C:2012:631.
6. T-553/23, *Latombe v Commission*, Application of 6 September 2023.
7. T-553/23 R, *Latombe v Commission*, Order of the President of the Court of 12 October 2023 (*Ordonnance*).
8. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, judgment of 6 October 2015, ECLI:EU:C:2015:650.
9. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, opinion of 23 September 2015, ECLI:EU:C:2015:627.
10. C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, judgment of 6 October 2020, ECLI:EU:C:2020:790.
11. C-203/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, judgment of 21 December 2016, ECLI:EU:C:2016:970.
12. C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, judgment of 16 December 2008, ECLI:EU:C:2008:727.

Academic sources:

1. Bowden C. et al., The US surveillance programmes and their impact on EU citizens' fundamental rights, European Parliament, Directorate-General for Internal Policies of the Union, Publications Office, 2013, available on https://data.europa.eu/doi/10.2861/34622.
2. Chu, V.S., Garvey, T.: "Executive Orders: Issuance, Modification, and Revocation", Congressional Research Service, 2014, available on https://sgp.fas.org/crs/misc/RS20846.pdf.
3. Colonna L.: "Europe Versus Facebook: An Imbroglio of EU Data Protection Issues", Data Protection on the Move, Current Developments in ICT and Privacy, Data Protection, Law, Governance and Technology: Series Issues in Privacy and Data Protection, Springer, 2016, pp. 25-50.
4. Fahey E. & Terpan F., "The Future of the EU-US Privacy Shield", The Routledge Research Handbook of Transatlantic Relations, 2023, Abingdon, United Kingdom, available on https://doi.org/10.4324/9781003283911, pp. 221-236.
5. Gao X., and Chen X., "Understanding the Evolution of Transatlantic Data Privacy Regimes: Ideas, Interests, and Institutions", Proceedings of the 2024 European

Interdisciplinary Cybersecurity Conference (EICC '24), Association for Computing Machinery, New York, USA, 2024, available on https://doi.org/10.1145/3655693.3655720, pp. 50–56.

6. Giacalone M., "Verso Schrems III ? Analisi del nuovo EU-US Data Privacy Framework", European Papers, Volume 8, No 1, 2023, pp. 149-157 available on https://doi.org/10.15166/2499-8249/644, pp. 149-157.
7. Granmar C.G., „A reality check of the Schrems saga", Nordic Journal of European Law, Volume 4 No. 2, 2021, available on https://ssrn.com/abstract=4000713, pp. 48-67.
8. Juliussen B. A., Kozyri E., Johansen D., Rui J. P., "The third country problem under the GDPR: enhancing protection of data transfers with technology", International Data Privacy Law, Volume 13, Issue 3, August 2023, available on https://doi.org/10.1093/idpl/ipad013, pp. 225–243.
9. Katulić T. and Vojković G., "From Safe Harbour to European Data Protection Reform", MIPRO 2016, 39th International Convention, 2016, available on https://www.researchgate.net/publication/305046213_From_Safe_Harbour_to_European_Data_Protection_Reform, pp. 1694-1698.
10. Laffranque J., „(Just) Give Me A Reason...", Juridica International, Volume 27, University of Tartu, Tartu, 2018, available on https://doi.org/10.12697/JI.2018.27.02, pp. 12-35.
11. Murphy M.H., „Assessing the implications of Schrems II for EU–US data flow", International & Comparative Law Quarterly, Volume 71, Issue 1, January 2022, available on: https://doi.org/10.1017/S0020589321000348, pp. 245- 262.
12. Naef T., Data Protection without Data Protectionism, The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law, European Yearbook of International Economic Law, EYIEL Monographs - Studies in European and International Economic Law, Springer, Volume 28, 2023, available on https://doi.org/10.1007/978-3-031-19893-9.
13. Neiazy V., „Invalidation of the EU–US Privacy Shield: impact on data protection and data security regarding the transfer of personal data to the United States", Int. Cybersecur. Law Rev. 2, 2021, available on https://doi.org/10.1365/s43439-021-00018-7, pp. 27-35.
14. Opdebeek I., i De Somer S., „The Duty to Give Reasons in the European Legal Area a Mechanism for Transparent and Accountable Administrative Decision-Making? A

Comparison of Belgian, Dutch, French and EU Administrative Law“, ROCZNIK ADMINISTRACJI PUBLICZNEJ 2016(2), Uniwersytet Jagielloński, Krakow.

15. Ortega Giménez A. “¿Y a la tercera va la vencida?. El nuevo marco transatlántico de privacidad de datos UE-EE.UU.”, Cuadernos de Derecho Transnacional, 16(1), 2024, available on: https://doi.org/10.20318/cdt.2024.8432, pp. 483-513.
16. Rodriguez S., „The United States of Surveillance: A Review of America’s Mass Surveillance Laws, Programs, and Oversight“, DHSI Conference & Colloquium, Volume 3, Iss. 2, 2021, available on https://doi.org/10.21428/f1f23564.f20c77b2.
17. Taylor M., Transatlantic Jurisdictional Conflicts in Data Protection Law, Cambridge University Press, 2023, available on http://dx.doi.org/10.1017/9781108784818.
18. Terpan F., “EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?”, European Papers, Volume 3, No 3, 2018, available on https://doi.org/10.15166/2499-8249/261, pp. 1045-1059.
19. Vrbljanac, D., “Managing Innovative Company’s Capital: The Case of Personal Data Transfer”, Zb. Prav. fak. Sveuč. u Rij., Vol. 39, No. 4, 2018, available on https://hrcak.srce.hr/file/318741, pp. 1779-1807.
20. Vrbljanac, D., “Personal Data Transfer to Third Countries – Disrupting the Even Flow?”, Athens Journal of Law - Volume 4, Issue 4, 2018, available on https://www.athensjournals.gr/law/2018-4-4-4-Vrbljanac.pdf, pp. 337-358.