LEXONOMICA
Vol. 16, No. 1, pp. 85–110, June 2024

LEXONOMICA

ANALYSING THE EU DATA PRIVACY IMPLICATIONS RESULTING FROM EXECUTIVE ORDER 14086: A LEGAL PERSPECTIVE

Accepted
25. 4. 2024

Revised
24. 6. 2024

Published
27. 6. 2024

ZORAN DIMOVIĆ
University in Maribor, Law faculty, Maribor, Slovenia
zoran.dimovic@student.um.si

CORRESPONDING AUTHOR
zoran.dimovic@student.um.si

Abstract The exchange of personal data between the EU and the USA has sparked intense debates and contentious discussions. This heightened attention can be attributed to significant disparities in data privacy regulations between the two regions, as well as mounting concerns surrounding the potential misuse of personal information by U.S. companies and government entities. In response to these concerns, the EU implemented the GDPR in 2018, which introduced stringent regulations aimed at safeguarding data privacy. Additionally, the GDPR imposed restrictions on the transfer of personal data to countries outside the EU that lack comparable data protection measures. One of the prominent legal challenges in this context relates to concerns over the adequacy of data protection in the USA, particularly in light of U.S. surveillance programs and the potential for government access to personal data.

Keywords
cross-border data transfer,
disparities in data privacy regulation,
GDPR implications,
human rights,
personal data transfer

https://doi.org/10.18690/lexonomica.16.1.85-110.2024

University of Maribor Press

1 Introduction

The flow of personal data from the European Union (EU) to the United States of America (USA; U.S.) has been a contentious issue in recent years. This is due to differences in the way data privacy is regulated in the two regions, as well as concerns over the potential misuse of personal data by U.S. companies and government agencies. The EU has long had strict regulations on data privacy, enshrined in the General Data Protection Regulation (GDPR)[1] which came into force back in May 2018. By coming into force, GDPR set a very high bar in privacy protection for individuals within EU member states (Dimović, 2023: 57-59). These regulations require companies to obtain explicit consent from individuals before collecting and processing their personal data,[2] as well as giving individuals the right to access and control their data. The GDPR also restricts the transfer of personal data to countries outside the EU that do not have similar regulations in place.[3]

The U.S, on the other hand, has a more fragmented approach to data privacy regulation and arguably the most significant difference in U.S. legislation (Halabi, 2022: 12) compared to the EU is the lack of a comprehensive data privacy law that applies to all U.S. companies and cover all types of private data. Those different acts cover different aspects of data privacy, like health data, data collected from children or financial information. There is no overarching federal law regulating data privacy, instead, data privacy is governed by a patchwork of state and sector-specific laws. The main federal laws are the Health Insurance Portability and Accountability Act (HIPAA)[4] and the Children's Online Privacy Protection Act (COPPA).[5] HIPAA is held by the US Department of Health and Human Services and sets rules on how personal health information may be used or shared, and how to file a complaint if you think your rights were violated. The COPPA, specifically articulated in CFR Article 16, Chapter 91, establishes a comprehensive framework for safeguarding children's online privacy. Enacted in 1998, COPPA delineates stringent definitions and mandates for operators of websites or online services targeted at children under

[1] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, pp. 1-88.
[2] Ibid, Recital 32.
[3] Ibid, Articles 44 through 49.
[4] Health information privacy. "U.S. Department of Health and Human Services." Accessed November 23, 2023. https://www.hhs.gov/hipaa/index.html.
[5] Children's Online Privacy Protection Rule ("COPPA"). 15. U.S.C. 6501-6505.

the age of 13. These provisions are designed to ensure that children's personal information is handled with utmost care, requiring operators to obtain verifiable parental consent before collecting any personal data from minors. Moreover, COPPA mandates the implementation of privacy policies that are clear, concise, and accessible to parents, outlining how children's information will be collected, used, and protected. This regulatory framework reflects ongoing efforts to address the unique privacy concerns associated with children's online activities, aiming to mitigate risks and uphold privacy rights in the digital age. Furthermore, there are also two other acts. One is Gramm-Leach-Bliley Act (GLBA)[6] prepared by the Federal Trade Commission (FTC) which have direct appliance to financial institutions and sets out standards and also responsibilities to protect the confidentiality and security of consumers' nonpublic personal information and to safeguard sensitive data.

Another pivotal legislation is the Federal Information Security Management Act (FISMA),[7] a federal statute mandating that federal agencies establish, document, and enforce comprehensive information security programs across their operations. FISMA, as amended in 2022,[8] represents a bipartisan effort to modernize and fortify federal information technology (IT) systems against contemporary cyber threats. This updated legislation adopts a forward-looking and strategic framework aimed at enhancing the resilience of federal information and systems, safeguarding them from unauthorized access, use, and disclosure.[9] FISMA 2022 emphasizes proactive measures to improve the readiness and response capabilities of federal agencies in addressing evolving cybersecurity challenges. It requires agencies to implement robust security controls, conduct regular risk assessments, and establish incident response protocols to promptly mitigate cyber incidents. Additionally, the legislation underscores the importance of continuous monitoring and evaluation of IT infrastructure to ensure compliance with security standards and to swiftly adapt to emerging threats. By promoting a comprehensive and adaptive approach to information security, FISMA 2022 aims to bolster the overall cybersecurity posture of federal agencies, fostering greater resilience and trust in the protection of sensitive

[6] Gramm-Leach-Bliley Act ("GLBA"). Pub. L. 106-102, 113.
[7] Federal Information Security Modernization Act of 2014. Pub. L. No. 113-283.
[8] Memorandum for the heads of executive departments and agencies. "Executive office of the president." Accessed November 22, 2023. https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-03-FY23-FISMA-Guidance-2.pdf.
[9] "America's Cyber Defence Agency." Accessed June 24, 2024. https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

government information. This legislative update reflects ongoing efforts to align federal cybersecurity practices with modern technological advancements and evolving threat landscapes, thereby enhancing the security and integrity of federal information systems. This fragmented approach to data privacy regulation has led to concerns over the adequacy of data privacy protections in the USA, particularly in light of high-profile data breaches and revelations about the extent of government surveillance programs. Namely in 2013, former National Security Agency (NSA) contractor Edward Snowden[10] revealed the extent of U.S. government surveillance, including the collection of data from internet and phone companies. This sparked concerns among EU citizens about the safety of their personal data when it is transferred to U.S. companies.

As will be seen throughout the article, the transfer of personal data from the EU to the U.S. is a multifaceted and contentious matter, carrying significant ramifications for individuals, businesses, and governments across the Atlantic. The existence of mechanisms like Standard Contractual Clauses (SCCs)[11] which arise from recitals 81, 109 and Article 28(7) of GDPR or Binding Corporate Rules (BCR)[12] arising from Articles 46 and 47 GDPR enables data transfers. Yet, doubts persist regarding the sufficiency of data protection regulations in the U.S. Undoubtedly, this issue is poised to remain a subject of ongoing deliberation and examination in the foreseeable future.

2 The Executive Order's Efforts to Expand Privacy Protections to Non-U.S. Persons: Progress or Inadequate Safeguards?

On July 26, 2000, the European Commission (EC) issued its initial adequacy decision regarding U.S. data privacy,[13] acknowledging the sufficiency of the privacy principles under the" US Safe Harbor framework",[14] which certain organizations could adhere

[10] He was a former computer intelligence consultant and »whistleblower" who leaked highly classified information from the NSA to the public in 2013. His disclosure revealed numerous global surveillance programs, many run by the NSA and Five Eyes intelligence alliance – and that prompted discussion about individual privacy.
[11] According to the GDPR, contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries and have to be pre-approved by the EC.
[12] Are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. The data protection authority in the EU will approve the BCRs in accordance with the consistency mechanisms set out in Article 63 of GDPR.
[13] 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 Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441). OJ L 215. 25. 8. 2000, pp 7-47.
[14] Ibid, see art. 1.

to. However, this decision was rendered invalid by the Court of Justice of the European Union (CJEU) in its "Schrems I" judgment.[15] CJEU ruled that "*legislation allowing public authorities unrestricted access to the content of electronic communications must be seen as undermining the core of the fundamental right to privacy*",[16] as enshrined in Article 7 of the Charter of Fundamental Rights of the European Union (Charter),[17] and also on Articles 8, 16, 47 and 52 thereof, referring to existing judgements.[18] Consequently, the "Safe Harbor" privacy principles were superseded by a new framework known as the EU-US Privacy Shield, widely recognized as the "Privacy Shield". Subsequently, on July 12, 2016, the Commission issued a second decision affirming the adequacy of the Privacy Shield's protective measures. This decision granted permission for seamless and unrestricted transfers of personal data to certified companies in the U.S. under the provisions of the Privacy Shield.

However, the CJEU rendered the aforementioned decision invalid in its ruling on "Schrems II."[19] The origins of the case lie in activist Maximilian Schrems' appeal to the Irish Data Protection Commissioner to invalidate the SCCs used by Facebook to transfer personal data to its headquarters in the U.S. Schrems argued that both during transit and storage in the US, the personal data could be accessed by U.S. intelligence agencies, potentially violating the GDPR and broader EU laws (Reinfeld, 2024: 8). The GDPR establishes a primary rule that prohibits transfers of personal data outside the EU and EEA unless adequate safeguards are in place. These safeguards include the EC's adequacy decisions where the EC evaluates and determines that a country's data protection laws are essentially equivalent to the GDPR following a thorough assessment of its national regulations. Additionally, prior to the" Schrems II" ruling, the mechanisms available for secure transfers outside the EU/EEA included the Privacy Shield, the EU SCC, and BCR (only for intra-group transfers). Article 49 also provides exemptions to the general principle, allowing for derogations when there are specific circumstances or legal grounds justifying the transfer to a country without a guaranteed adequate level of protection.

[15] Judgment of 6 October 2015, *Maximilian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:650.
[16] Ibid, see para. 94.
[17] EU Charter of Fundamental Rights: Charter of Fundamental Rights of the European Union, OJ 2010 C 83/ 389.
[18] Paragraph 39 of CJEU judgements C-293/12 and C-594/12, *Digital Rights Ireland and Others*.
[19] Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, C-311/18, EU:C:2020:559.

The CJEU reached this determination after a meticulous examination of U.S. surveillance laws, notably Section 702 of the Foreign Intelligence Surveillance Act (FISA)[20] and Executive Order 12333,[21] in conjunction with the EU-U.S. Privacy Shield decision itself. Upon this comprehensive review, the CJEU concluded that these U.S. laws lack sufficient limitations and effective oversight regarding public authorities' access to personal data originating from the EU. Furthermore, the CJEU found that the Privacy Shield fails to afford EU individuals actionable and effective rights before the courts against such public authorities. Specifically, the CJEU underscored that the Privacy Shield Ombudsman is incapable of adequately addressing these deficiencies. Consequently, the CJEU held that the Privacy Shield framework is incompatible with the safeguards and requirements mandated by EU law. This judgment was grounded in the inadequacies of the Privacy Shield to protect fundamental rights as required by EU standards, particularly the essence of the fundamental right to privacy as enshrined in Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) (Reinfeld, 2024: 22). This ruling underscores the need for robust data protection measures that align with EU legal principles and adequately safeguard individuals' privacy rights against broad surveillance practices.

In its assessment, the CJEU highlighted the incompatibility of the Privacy Shield decision with Article 45(1) of the GDPR, taking into account the stipulations of Articles 7, 8, and 47 of the Charter. The CJEU expressed significant concerns regarding the extensive access to data afforded to U.S. surveillance authorities and pinpointed deficiencies in the oversight mechanisms of the Privacy Shield. Consequently, the CJEU determined that these elements failed to provide adequate legal protection for EU citizens. As a result of this judgment, the U.S. and the EC initiated negotiations to develop a framework that would ensure personal data transfers to the U.S. maintain an essentially equivalent level of protection as required by the CJEU's "Schrems II" ruling. This new framework aims to address the identified shortcomings and align with the stringent data protection standards upheld by EU law, thereby ensuring that the fundamental rights to privacy and data protection of EU citizens are fully respected in transatlantic data exchanges.

[20] The Foreign Intelligence Surveillance Act of 1978 (FISA). 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871. 1978.
[21] Executive Order 12333. "Ministry of defense." Accessed November 21, 2023. https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf

This effort led to significant development, with the EC and the U.S. reaching a preliminary agreement for a new EU-US Data Privacy Framework called the Data Privacy Framework (DPF)[22] by the end of March 2022. The DPF represents an updated version of the framework applicable to certified commercial entities involved in processing personal data transferred from the EU. It represents an important milestone in safeguarding data privacy. Considering data protection and privacy issues stated in the Schrems II ruling and DPF, President Biden made a noteworthy move by endorsing Executive Order 14086 (EO)[23] that introduces more stringent constraints on surveillance programs within the U.S. Simultaneously, the order establishes a new mechanism for individuals residing outside the country to seek recourse. This includes, in his opinion, two core components: proportionality (Lindsay, 2018: 49-84) in intelligence gathering and the increased role of the U.S. Department of Justice (DOJ) with the Data Protection Review Court (DPRC). The Executive Order 14086 includes three main components: commercial data protection principles to which U.S. organizations may self-certify, a presidential EO and DOJ regulations. Perhaps the most important part is the newly specified term of personal data under the commercial principles, which links directly to GDPR and not to Directive 1995 Data Protection Regulation[24] as it was in the Privacy Shield. These efforts collectively aim to address the necessity and proportionality constraints[25] on U.S. surveillance programs, as well as the insufficient redress mechanisms available to challenge unlawful government surveillance. Both the substantive content and the legal framework of these components are critical under the CJEU's essential equivalence test.[26] The necessity and proportionality principles are fundamental to ensuring that any surveillance activities conducted by U.S. authorities are strictly limited to what is essential for achieving legitimate objectives and are balanced against the intrusion on individuals' privacy rights. This necessitates a thorough assessment of the justifications for surveillance, the scope of data

[22] Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision. "European Commission." Accessed November 21, 2023. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632

[23] Executive Order 14046. "Presidential Documents." Accessed November 20, 2023. https://ofac.treasury.gov/media/913011/download?inline.

[24] 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 L 281, pp. 31-50.

[25] As in Schrems II ruling »[n]either Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programs based on those provisions cannot be regarded as limited to what is strictly necessary."

[26] For more see International Association of Privacy Professionals. Accessed June 24, 2024. https://iapp.org/

collection, and the specific measures in place to minimize any adverse impact on privacy. Equally important is the establishment of robust redress mechanisms that enable individuals to effectively challenge and seek remedies for unlawful surveillance practices. This includes ensuring that individuals have access to independent judicial oversight and the ability to obtain meaningful redress, thereby reinforcing the protection of their fundamental rights. Under the CJEU's essential equivalence test, it is not enough for the U.S. to merely articulate these principles; they must be embedded within a legal framework that provides tangible, enforceable protections. This involves creating clear legal standards, implementing rigorous oversight mechanisms, and guaranteeing that individuals have actionable rights. In essence, both the material content and the legal architecture of these reforms are crucial in demonstrating that the protections afforded to EU citizens' personal data in the U.S. are essentially equivalent to those guaranteed under EU law. This comprehensive approach seeks to align U.S. surveillance practices with the stringent data protection standards upheld by the EU, thereby facilitating a secure and legally sound framework for transatlantic data transfers.

In terms of content, the EO establishes substantial limitations on surveillance programs by explicitly requiring the adherence to principles of necessity and proportionality (Joel, 2023: 21). Furthermore, it provides an explanation of what these requirements entail and outlines oversight mechanisms to ensure intelligence agencies comply with the newly defined rules. The order articulates the following in Sec. 2 (a)(i)(A): "*signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and (B) signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.*"[27]

[27] Refer to Sec. 2(a)(i)(A).

These safeguards encompass various dimensions, including the scope of signals intelligence collection, its permissible uses and sharing protocols, and the duration for which the collected data can be retained. The Executive Order (EO) delineates 12 specified "legitimate objectives," such as the protection of personnel within the U.S. or its allies, which signals intelligence activities must adhere to. Additionally, the EO identifies 4 prohibited objectives, such as impeding or restraining criticism, dissent, or the free expression of ideas or political opinions.[28] The EO, in conjunction with DOJ regulations, establishes a two-tiered redress mechanism, featuring the newly instituted DPRC. This system is specifically designed to address the second fundamental requirement of essential equivalence, which the CJEU identified as deficient in both the Privacy Shield and the U.S. legal framework. The CJEU's ruling highlighted a "gap in judicial protection" regarding interferences with intelligence programs, noting that neither Presidential Policy Directive 28 (PPD-28) nor Executive Order 12333 provide data subjects with actionable rights in court against U.S. authorities, thus depriving them of an effective remedy.[29] Furthermore, the CJEU clarified that the Privacy Shield Ombudsman does not adequately address these deficiencies, as it lacks the authority to issue binding decisions on intelligence authorities and is not independent from the executive branch, given that the Ombudsman may be dismissed. The EO and the DPRC aim to rectify these shortcomings by instituting mechanisms that offer EU data subjects more robust protections and avenues for redress, aligning with the stringent standards required by the CJEU's essential equivalence test. By specifying clear objectives and prohibitions for signals intelligence activities and establishing a credible redress mechanism, the EO seeks to provide a legal structure that ensures U.S. surveillance practices are both necessary and proportionate, thereby offering a level of data protection that is fundamentally equivalent to that provided under EU law. This comprehensive approach is intended to facilitate secure and compliant transatlantic data transfers, ensuring that the fundamental rights to privacy and civil liberties are upheld in line with EU standards.

While this EO aims to replace the outdated Privacy Shield initiative, it is doubtful that it will fully meet the legal requirements set by the EU to ensure privacy protection. The current concern revolves around whether this repetitive pattern of

[28] Refer to Section 2(b).
[29] Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, C-311/18, EU:C:2020:559.

dismantling and rebuilding will continue indefinitely or instead act as a foundation for wider multilateral cooperation or even advancements in U.S. federal legislation. The objective would be to establish commercial data protections that are universally binding for individuals, irrespective of their nationality or place of residence, akin to the standards set for their national security counterparts. So there seems to be progress to make data protection on trans-Atlantic data flow more concise, however, the safeguards are yet not adequate to sustain EC or CJEU tests.[30]

3 Trans-Atlantic data flow protection and privacy redress mechanisms

There are few Trans-Atlantic data flow protection mechanisms, which guarantee data flow protection between the EU and the U.S. One such mechanisms are Standard Contractual Clauses (SCCs), which are pre-approved contracts that set out data protection obligations for companies (Gerke, 2023: 372). SCCs have been used for many years as a way of transferring data to countries outside the EU, and they remain a popular mechanism for transferring data to the U.S. However, there are concerns that SCCs may not offer sufficient protection for personal data in light of the EU Court of Justice ruling. Other safeguards such as BCR can be found as per Article 47(1) of GDPR, to which it can have influence either on the controller in accordance with Article 79 of GDPR, DPO by Article 37 of GDPR or to processor according to Article 22 of GDPR.

Amidst the prevailing uncertainty, the EC has emphasized the necessity for companies to uphold robust obligations regarding the processing of data transferred from the EU. Therefore, companies should carefully evaluate whether they wish to incorporate the Transatlantic Data Privacy Framework (TADPF) as one of their data transfer solutions (McCabe, 2022: 18). If they opt for TADPF, companies should review and familiarize themselves with the Privacy Shield Principles, upon which the TADPF is based. They should assess their ability to comply with the extensive requirements outlined in the principles, covering aspects such as notice, choice, onward transfers, security, access, recourse, enforcement, and liability. While the specific TADPF compliance requirements are not yet fully defined, it is reasonable to anticipate similarities with those of the Privacy Shield. In the interim, until EC's

[30] Competences of the Court of Justice of the European Union. "European Parliament." Accessed November 21, 2023. https://www.europarl.europa.eu/factsheets/en/sheet/12/competences-of-the-court-of-justice-of-the-european-union.

adequate final decision is made and until the TADPF is finalized, companies should continue utilizing approved data transfer mechanisms such as BCR or SCCs. It is also advisable to conduct transfer impact assessments (TIAs)[31] as needed. TIAs help identify potential risks to the security of the transferred personal data and determine whether additional security measures are necessary, considering the laws of the importing country. For U.S.-related TIAs, the enhanced checks and balances introduced by EO should be considered as part of a comprehensive risk assessment. Companies who intend to rely on the TADPF adequacy decision as a valid transfer mechanism will also need to be certified by the Department of Commerce under the new TADPF. In anticipation of this certification process, companies can take preliminary steps by updating their data maps, inventories, and compiling the necessary policies and procedures that require revisions (Marconi, 2023: 5). Companies with an active Privacy Shield certification may consider renewing it to potentially facilitate the transition to TADPF registration from an administrative perspective. It should be noted that the TADPF may not serve as a long-term solution due to potential administrative and legal challenges in both the EU and the U.S. Nevertheless, companies can presently benefit from the TADPF by utilizing it as a transfer mechanism until its adequacy or legality is determined.

As for Privacy redress mechanisms in conjunction, Section 3 of the EO and the regulation DOJ establish a two-tier system for addressing grievances. This system processes" qualifying complaints" that are transmitted from" qualifying states" concerning U.S. signals intelligence activities that may involve a" covered violation" of U.S. law and only public authorities from a qualifying state are authorized to submit complaints on behalf of individuals (complainants) against U.S. intelligence activities that impact the privacy and civil liberties interests of the complainant, particularly regarding data transferred to the U.S. (Mildebrath, 2022: 6). These complaints may allege violations of specific elements of U.S. law, including the executive order itself (Determan, 2023: 126). To facilitate the redress mechanism, the Attorney General (AG) has the authority to designate a foreign country or regional economic integration organization (REIO) as a qualifying state.

[31] A transfer impact assessment clarifies your organization's risks for transferring EU residents' data to countries without adequacy under the GDPR. It is a questionnaire that needs to be completed by either party to the data transfer i.e., data importer or data exporter.

Furthermore, the Executive Order institutes a bifurcated redress framework for individuals whose personal data may have been intercepted by intelligence agencies. The initial tier comprises an investigation by a Civil Liberties Protection Officer (CLPO), who is tasked with examining, reviewing, and, if warranted, mandating remedial actions for qualifying grievances. A grievance is deemed qualifying if it meets the following stringent criteria:

a) It alleges a covered violation related to the personal information of the complainant—a natural person—reasonably presumed to have been transferred to the United States from a qualifying state.
b) It provides the requisite foundational information for review. This includes, but is not limited to, evidence supporting the claim of a covered violation, without necessarily proving that the complainant's data has indeed been subjected to U.S. signals intelligence activities. Furthermore, it must specify the nature of the relief sought, the specific channels through which the complainant's personal data is believed to have been transmitted to the United States, the identities of the U.S. government entities implicated in the alleged violation (if known), and any other remedial measures pursued by the complainant along with the responses received from such measures.
c) The complaint must not be frivolous, vexatious, or made in bad faith.
d) It must be filed by the complainant acting in their personal capacity, and not as a representative of any governmental, non-governmental, or intergovernmental organization.
e) It must be submitted by the appropriate public authority in a qualifying state, which has authenticated the identity of the complainant and confirmed that the complaint meets the stipulated conditions.

This comprehensive procedural mechanism ensures that individuals have a structured and rigorous pathway to seek redress for potential violations of their personal data privacy by intelligence entities. Despite its intentions, the new redress mechanism exhibits several critical deficiencies. Primarily, EU data subjects face significant barriers to federal judicial recourse due to multiple layers of secrecy and the stringent requirement for litigants to demonstrate actual injuries resulting from privacy breaches to establish standing in court. Consequently, no civil lawsuit has successfully challenged the legality of surveillance under Section 702 of the FISA or EO 12333, nor has any U.S. court rendered an opinion on the lawfulness of such

surveillance activities. Further implications are evident in the structure and operation of the redress mechanism. Firstly, the independence of both tiers of redress is compromised by their integration within the executive branch. Fact-finding is conducted by an ODNI office rather than an independent court and also the DPRC judges are appointed by the Attorney General, not by an autonomous third-party agency. Furthermore, there are no restrictions on the President's authority to dismiss these judges, and the President also has the power to overrule the court's decisions. Moreover, the dependence of DPRC judges on the executive branch for the potential renewal of their four-year terms may influence their impartiality, potentially leading to biased judgments (Mildebrath, 2022: 7). Secondly, the categorical confidentiality of findings and evidence at the initial redress stage impedes complainants' access to pertinent information, raising concerns about the fundamental fairness of the redress process. Thirdly, the executive order allows the redress bodies to issue generic summary responses that neither confirm nor deny surveillance activities and provide no substantive details on the facts and merits of the case. This lack of transparency hampers the complainant's ability to pursue a well-informed appeal. Fourthly, the absence of a timely obligation to notify surveillance targets ex post about surveillance measures (notification duties) means that Europeans are seldom aware of the need to file a complaint or appeal, thereby limiting their ability to seek remedies. Lastly, the executive order does not address the U.S. government's acquisition of bulk data, leaving a significant gap in the protection of personal data against mass surveillance practices.[32]

These shortcomings collectively undermine the efficacy and integrity of the redress mechanism, casting doubt on its ability to provide meaningful protection for individuals' privacy rights in the context of intelligence surveillance.

Nonetheless, the transference of personal data from the EU to U.S.-based companies is contingent upon strict compliance with established frameworks. Specifically, U.S. companies must adhere to one of the following protocols to lawfully receive such data:

[32] "European Parliament, Think Tank, Briefing research, The future of data protection and privacy: How the European Parliament is responding to citizens' expectations, 27-04-2022" Accessed June 24, 2024. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)729396

a.) EU-U.S. Privacy Shield Program: Companies may join this framework, which ensures compliance with EU data protection standards and provides mechanisms for redress.
b.) Appropriate Safeguards: Alternatively, companies can implement appropriate safeguards, such as SCC's or BCR's. These safeguards establish legally binding obligations to protect personal data and ensure its secure transfer in accordance with the GDPR.
c.) GDPR Derogations: As delineated in Article 49 of the GDPR, companies may also rely on specific derogations. These exceptions permit data transfer under particular conditions, such as explicit consent from the data subject, necessary transfers for the performance of a contract, or transfers required for important reasons of public interest.

Each of these mechanisms is designed to ensure that personal data transferred from the EU to the U.S. is afforded a level of protection consistent with EU privacy standards, thereby safeguarding the rights and freedoms of data subjects. Failure to comply with these stringent requirements can result in significant legal repercussions, including fines and restrictions on data processing activities.

4 Key Differences: GDPR Principles vs. Executive Order Provisions

The principles of" necessity" and" proportionality" are closely intertwined in both EU law and Article 8 of the European Convention on Human Rights (ECHR).[33] Article 51 of the Charter states that limitations can only be imposed if they are necessary and genuinely serve objectives of general interest, subject to the principle of proportionality. The European Court of Human Rights (ECtHR) has determined that the term" necessary" includes the concept of proportionality. In other words, a restriction on a Convention Right cannot be considered" necessary in a democratic society" unless it is proportionate to the legitimate aim pursued.[34] The EO seeks to distinguish these concepts and express them in a manner that aligns with U.S. legal traditions, mainly as per the Privacy act for U.S. citizens (Zemer, 2021: 684).

[33] European Convention on Human Rights. Rome, 4. XI. 1950.
[34] Guide on Article 8 of the European Convention on Human Rights. "European Court of Human Rights." Accessed November 22, 2023. https://www.echr.coe.int/documents/guide_art_8_eng.pdf

Although the GDPR in the EU provides a robust framework for protecting personal data, the level of protection can be compromised when transferring or remotely accessing data to and from third countries (countries outside the EU or EEA). This is due to conflicting national laws and international obligations in these third countries that cannot be reconciled with the GDPR, resulting in a lower level of data protection. The U.S., in particular, grants authorities extensive access rights to data, which may require a company to disclose personal data even if it is prohibited under the GDPR. Consequently, the GDPR imposes additional requirements for international data transfers.[35]

The fundamental principles of the GDPR, rooted in the longstanding tradition of protecting human rights within the EU, include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. In comparison to the EO, it is worth noting that the GDPR mandates individuals to give their consent (opt-in) before businesses can collect their data, while there is no such opt-in requirement in the EO or the California Consumer Privacy Act (CCPA),[36] which closely resembles the GDPR in the U.S. To ensure adequate protection in specific countries, the EC evaluates the level of data protection in those countries and issues" adequacy decisions"[37] if the level is deemed equivalent to that within the EU. These decisions simplify the process of transferring personal data to those countries. A list of these third countries can be found, but the U.S. is not included in that list (Propp, 2023: 9).

The EO reinforces the principle of "proportionality" by mandating that signals intelligence activities be conducted only to the extent and in a manner commensurate with the validated intelligence priorities for which they have been authorized. This mandate aims to ensure an appropriate equilibrium between the significance of the intelligence objectives pursued and the impact on the privacy and civil liberties of all individuals, regardless of their nationality or place of residence. Specifically, the EO stipulates that the proportionality principle must guide all signals intelligence operations, thereby emphasizing that the scope and intensity of these activities must be justified by the importance of the intelligence needs they serve. This requirement

[35] Art. 44 GDPR et seq.
[36] Assembly Bill No. 375. (2018). Chau, Privacy. "California legislative information." Accessed November 15, 2023. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
[37] Art. 45 GDPR.

underscores the necessity of a balanced approach, where the pursuit of national security and intelligence objectives does not unduly compromise individual privacy rights and civil liberties. Furthermore, this provision aligns with the directives set forth in section 2(a)(ii)(B) of the EO, which calls for a meticulous consideration of privacy and civil liberties. It highlights the imperative of integrating proportionality into the decision-making processes governing signals intelligence, ensuring that every action taken is not only effective in meeting intelligence goals but also mindful of the inherent rights and freedoms of individuals. By embedding this principle within the operational framework, the EO seeks to foster a responsible and ethical approach to intelligence gathering, one that respects the delicate balance between security imperatives and personal privacy.

The concept of "proportionality" is not explicitly codified in U.S. surveillance law, despite its significant legal import in other domains of U.S. jurisprudence. In U.S. constitutional law, proportionality is embedded in various doctrines, incorporating elements of the "structured proportionality review" frequently employed in international constitutional frameworks. This review often entails assessments of "narrow tailoring" or the exploration of "less restrictive alternatives," akin to the rigorous analysis employed in the U.S. strict scrutiny standard (Jackson, 2015: 3113). Under the strict scrutiny standard, any governmental action that impinges upon "fundamental rights" must demonstrate that such action or legislation is necessary, or "narrowly tailored," to achieve a compelling governmental interest. This principle requires the government to prove that there are no less restrictive means available to achieve the same objective. The scrutiny ensures that any infringement on fundamental rights is minimized and justified by an overriding public interest. This rigorous analysis is well-understood and frequently utilized by U.S. legal practitioners. It necessitates a meticulous balancing act, ensuring that the government's interest in security or other compelling needs does not disproportionately infringe on individual rights and liberties. Thus, while the term "proportionality" itself may not be explicitly mentioned in U.S. surveillance law, the underlying principles are ingrained in the broader constitutional doctrine, shaping the legal landscape in ways that promote a balance between governmental powers and individual freedoms.

As can be seen EU main principles in EO were not followed sufficiently which may led to inadequate guarantees of data privacy under EO.

5 Implications for Data Transfers and Compliance

The EO exhibits two notable deficiencies that may precipitate legal conflicts under EU law, starting firstly, the EO subjects U.S. signals intelligence (SIGINT)[38] activities, consistent with the application scope of Presidential Policy Directive 28 (PPD-28),[39] to additional safeguards. However, similar to PPD-28, the EO lacks a precise definition of signals intelligence. This omission raises concerns about potential inconsistencies in application and ambiguities in scope, mirroring the issues observed with PPD-28, which the EO predominantly supersedes (Mildebrath, 2022: 9). The ODNI characterizes signals intelligence as intelligence gathered from intercepted signals. This encompasses communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence. According to the NSA, signals intelligence may be derived from a variety of sources, including communication systems, radar systems, and weapon systems.[40]

The absence of a clear definition within the EO could lead to variable interpretations and applications across different intelligence agencies, potentially undermining the uniformity and predictability required for robust legal oversight. This lack of specificity may also hinder the EO's compliance with the stringent data protection standards mandated by EU law, particularly in light of the GDPR and the Schrems II decision by the CJEU. These legal instruments emphasize the necessity for clear, precise, and transparent data processing practices, especially concerning transatlantic data flows and the protection of EU citizens' personal data. Thus, the EO's vagueness regarding the scope and definition of signals intelligence poses significant risks for legal compliance and could engender disputes with EU authorities, further complicating the legal landscape for U.S. intelligence operations involving data from EU residents. This uncertainty underscores the need for more explicit definitions and consistent application protocols to mitigate potential legal challenges and ensure adherence to international data protection standards.

---

[38] Signals Intelligence (SIGINT) Overview. "National Security Agency/Central Security Service." Accessed November 20, 2023. https://www.nsa.gov/Signals-Intelligence/Overview/

[39] Presidential Policy Directive 28 (PPD-28) Signals Intelligence Activities. "Homeland Security." Accessed November 16, 2023. https://www.dhs.gov/publication/presidential-policy-directive-28-ppd-28-signals-intelligence-activities.

[40] "European Parliament, Think Tank, Briefing research, The future of data protection and privacy: How the European Parliament is responding to citizens' expectations, 27-04-2022" Accessed June 24, 2024. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)729396

Section 2 of the EO stipulates that signals intelligence may be collected for the pursuit of one or more of twelve legitimate objectives and explicitly prohibits its use for five specific purposes (Rubinstein, 2022: 64). The European Parliamentary Research Service (EPRS) has indicated that the President retains the authority to (secretly) update the list of legitimate objectives and signals intelligence activities must be authorized and conducted in accordance with principles of authorization, necessity, proportionality, and oversight (Mildebrath, 2022: 9). The principles of necessity and proportionality require that intelligence activities are subject to appropriate safeguards, ensuring they are conducted only when necessary and in a manner proportionate to advancing a "validated intelligence priority." The necessity determination is based on a reasonable assessment of all relevant factors, while the proportionality test aims to balance the significance of the intelligence priority against the impact on the privacy and civil liberties of all individuals (Mildebrath, 2022: 9).

The NIPF,[41] which outlines the validated intelligence priorities, is confidential, but much of its content is reflected in the ODNI's unclassified annual WTA.[42] Subsection (c) of Section 2 establishes privacy and civil liberties safeguards designed to fulfill the principles of necessity, proportionality, and oversight. It sets forth rules for (i) the collection of signals intelligence, (ii) the bulk collection and use of signals intelligence, (iii) the handling of personal information collected, and (iv and v) the updating, publication, and review of certain policies and procedures within the Intelligence Community, which comprises eighteen organizations.[43]

Under the stipulated privacy and civil liberties safeguards, signals intelligence collection activities must be "as tailored as feasible" to advance a validated intelligence priority, ensuring minimal adverse impact on privacy and civil liberties. This terminology diverges from the conventional proportionality principle, which emphasizes a balanced approach between the significance of intelligence objectives and the protection of individual rights. Ideally, bulk collection should be authorized

[41] The national intelligence priorities framework (NIPF). Intelligence Community Directive 204. Office of the Director of National Intelligence.
[42] Worldwide Threat Assessment. Annual threat assessment of the U.S. intelligence community. "Office of the Director of National Intelligence." Accessed November 21, 2023.
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
[43] "European Parliament, Think Tank, Briefing research, The future of data protection and privacy: How the European Parliament is responding to citizens' expectations, 27-04-2022" Accessed June 24, 2024. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)729396

primarily when targeted collection methods are insufficient to obtain the required information reasonably. The scope of bulk collection is further constrained to six designated objectives, including safeguarding against terrorism, espionage, and cybersecurity threats and these restrictions aim to ensure that the expansive reach of bulk collection is justified only by critical and specific intelligence needs, thereby preventing unwarranted intrusions into personal privacy. Moreover, the authorization for bulk collection necessitates a rigorous assessment to confirm that such measures are indispensable and that no less invasive alternatives are available. This assessment is crucial to uphold the principles of necessity and proportionality, ensuring that intelligence operations are conducted with the utmost respect for privacy and civil liberties. In addition, the implementation of these safeguards requires robust oversight mechanisms to monitor compliance and address any potential abuses (Schwartz, 2013: 1989). The oversight framework is designed to ensure transparency and accountability within intelligence operations, providing a check against disproportionate or unjustified data collection practices. By embedding these principles and safeguards within the operational protocols, the EO seeks to align signals intelligence activities with the highest standards of privacy protection and civil liberties.

When managing personal data obtained through signals intelligence, the Intelligence Community (IC) is mandated to institute protocols for data minimization, robust data security measures, ensuring data quality, managing access permissions for bulk collection queries, and maintaining comprehensive documentation. These measures are essential to mitigate privacy risks and uphold the integrity of collected information. Furthermore, leaders of IC organizations are directed to regularly update policies and procedures to effectively enforce these privacy and civil liberties safeguards. These updates must be publicly disclosed within one year from the issuance of the Executive Order (EO), promoting transparency and accountability in intelligence operations. The Privacy and Civil Liberties Oversight Board (PCLOB)[44] is encouraged to conduct thorough reviews of these updates, ensuring they align with legal and ethical standards. Additionally, Section 2(d) of the EO reinforces existing oversight mechanisms, ensuring stringent scrutiny of signals intelligence activities. This oversight framework is pivotal in safeguarding the privacy

[44] U.S. Privacy and Civil Liberties. "U.S. Privacy and civil liberties Oversight board." Accessed November 20, 2023. https://www.pclob.gov/

and civil liberties of individuals, maintaining a balance between national security imperatives and individual rights in the realm of intelligence gathering.

Furthermore, the U.S. has not yet achieved a level of data protection that is deemed essentially equivalent to that of the EU. This is evidenced by the EO allowing for an implementation period of up to one year, with actual implementation expected to span several months (Chander, 2023: 83-85). The transient and reversible nature of executive orders raises concerns regarding their ability to provide enduring legal certainty. Moreover, uncertainties persist regarding the interaction between the EO and the Cloud Act,[45] complicating the regulatory landscape further. Additionally, disparities in the interpretation of proportionality between the EU and the U.S. are notable, particularly concerning permissions for bulk surveillance, which may not meet the standards set by the CJEU. Addressing these challenges requires harmonizing regulatory frameworks and bridging gaps in understanding between transatlantic partners. Achieving a mutually recognized level of data protection is essential for facilitating secure and compliant data transfers between the EU and the U.S., while also respecting fundamental rights and legal principles on both sides of the Atlantic.

The aforementioned provisions apply universally to all forms of signals intelligence operations, encompassing both "targeted" and "bulk collection" methodologies. These regulations and safeguards are designed to ensure that regardless of the method used to gather signals intelligence, stringent principles of authorization, necessity, proportionality, and oversight are consistently upheld. Targeted signals intelligence involves the focused collection of data on specific individuals, entities, or activities of interest. It requires precise authorization and adherence to strict guidelines to minimize collateral impact on non-targeted individuals' privacy and civil liberties. In contrast, bulk collection entails the indiscriminate gathering of large volumes of data, which necessitates even more stringent oversight and justification. The EO 12333, authorized by PPD-28, mandates that bulk collection can only be justified when targeted collection methods are inadequate for obtaining necessary intelligence, and it must adhere to predefined objectives such as countering terrorism, espionage, and cybersecurity threats, as already addressed. By applying these regulations comprehensively across all types of signals intelligence activities,

[45] Cloud Act. H.R. 4943.

the EO aims to balance national security imperatives with the protection of individual privacy and civil liberties. This approach seeks to ensure that intelligence operations are conducted in a manner that is both effective and respectful of legal and ethical standards, fostering transparency and accountability within the IC.

Additionally, it is noteworthy that the redress mechanism outlined in the EO operates under conditions of confidentiality, lacking a mandatory notification requirement for complainants regarding the processing of their personal data. This omission undermines their rights to access and rectify their data, which are fundamental principles under data protection laws.[46] Furthermore, concerns have been raised about the impartiality and independence of the DPRC board established by the EO. The complainant is represented by a "special advocate" appointed by the DPRC, without a mandate for independent representation, thus potentially compromising the fairness of the process under the principles enshrined in the Charter (Mildebrath, 2022: 9). Moreover, the absence of a federal appeal route for data subjects further limits avenues for recourse, potentially hindering the effectiveness of the redress mechanism. These shortcomings highlight significant challenges in aligning the EO's provisions with international standards of privacy, fairness, and transparency. These issues underscore the need for robust safeguards and procedural enhancements to ensure that redress mechanisms effectively protect individuals' rights while maintaining national security imperatives. Addressing these concerns is crucial for fostering trust and compliance in cross-border data transfers and intelligence activities.

6 Summaries of key findings and insights

With the implementation of the EO in the United States, the EC is now empowered to initiate the drafting of an adequacy decision to assess whether the updated U.S. data protection standards align with the essential equivalence required by EU regulations. This evaluative process involves soliciting a non-binding opinion from the EDPB board and securing approval from the Article 93 Committee, which comprises representatives from EU Member States ("comitology procedure") (Mildebrath, 2022: 7). Additionally, the EP and the EC are kept informed of

[46] "European Parliament, Think Tank, Briefing research, The future of data protection and privacy: How the European Parliament is responding to citizens' expectations, 27-04-2022" Accessed June 24, 2024. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)729396

committee proceedings and retain the authority to request adjustments to the adequacy decision under Article 45 of the GDPR. To bolster transparency and accountability, it is essential to define scenario-specific EU standards, identify the internal factors[47] influencing these standards, and delineate any flexibility inherent in the CJEU concept of "essential equivalence."[48] This framework ensures a nuanced understanding of how EU standards apply across different contexts and accommodate evolving legal interpretations over time. The EO introduces stringent restrictions on electronic surveillance conducted by U.S. intelligence agencies, aiming to safeguard against indiscriminate data collection practices. It establishes robust mechanisms for EU citizens to file complaints concerning the alleged unlawful processing of their personal data by U.S. authorities, thereby enhancing legal recourse and protection of individual rights. Furthermore, the EO lays the foundation for a forthcoming DPF aimed at facilitating secure and legally compliant data transfers between the EU and the U.S. This DPF framework underscores that any signals intelligence collection must be substantiated as essential and proportionate to uphold U.S. national security imperatives while concurrently safeguarding fundamental rights to privacy and civil liberties. The DPF represents a strategic initiative to harmonize data protection standards across transatlantic borders, ensuring robust mechanisms are in place to govern how personal data is collected, processed, and transferred between the EU and the U.S. Central to this framework is the principle that signals intelligence activities must align with stringent

[47] E.g. In assessing EU standards, several factors are pivotal for determining their relevance: firstly, the adoption of common minimum standards implemented at the national level across EU member states; secondly, adherence to standards set forth in the ECHR, which serve as a foundational framework for human rights protection across Europe; and thirdly, the development and application of distinct EU standards tailored to meet specific regional needs and challenges. Common minimum standards implemented nationally ensure a baseline level of protection for individuals' rights and freedoms within each member state, contributing to consistency and coherence in the application of EU law. These standards often encompass fundamental principles such as data protection, privacy rights, and procedural fairness in legal matters. The ECHR establishes a comprehensive set of rights and freedoms that member states are obligated to uphold, providing a benchmark against which EU standards are evaluated. These rights encompass civil and political liberties, including the right to privacy, freedom of expression, and the right to a fair trial, among others. Furthermore, the EU develops its own set of standards that address specific regional challenges and reflect the values and priorities of its member states. These standards may encompass regulatory frameworks such as the GDPR, which harmonizes data protection laws across the EU and ensures a high level of protection for personal data. Understanding these factors is crucial for comprehending the complexity and evolution of EU standards over time. It underscores the EU's commitment to promoting and safeguarding fundamental rights and freedoms while fostering cooperation and coherence in legal and regulatory frameworks across member states. By considering these factors, policymakers can ensure that EU standards remain robust, adaptable, and responsive to emerging challenges in a rapidly evolving global landscape.

[48] Within the EU, data subjects encounter diverse avenues for seeking redress, which vary based on the surveillance context and the specific Member State involved. Comparing these redress mechanisms reveals differing advantages and limitations, prompting an evaluation to determine their potential equivalence in efficacy and fairness. This comparative analysis aims to assess whether these mechanisms effectively uphold fundamental rights across different jurisdictions within the EU.

criteria of necessity and proportionality. This ensures that such activities are conducted only when deemed vital for national security purposes and are proportionate to the risks posed, thereby mitigating potential impacts on privacy rights and civil liberties. Moreover, the DPF aims to establish clear guidelines and procedural safeguards that uphold the principles of transparency, accountability, and legality in intelligence gathering practices. By fostering mutual understanding and compliance with internationally recognized standards, the framework seeks to foster trust and facilitate uninterrupted data flows essential for economic and security cooperation between the EU and the U.S. However, challenges persist in reconciling differing interpretations of privacy and surveillance practices between the EU and the U.S., highlighting the need for ongoing dialogue and adaptation of regulatory frameworks to ensure mutual respect for rights and obligations. As the DPF progresses towards implementation, stakeholders must collaborate to address these complexities and achieve a balanced approach that upholds both national security imperatives and individual rights within the digital age.

Despite the heightened scrutiny and restrictions imposed on U.S. surveillance programs, the EO retains provisions allowing for bulk collection of personal data in specified circumstances. This provision reflects ongoing debates and considerations regarding the balance between maintaining robust national security capabilities and protecting the privacy rights of individuals, particularly in the context of transatlantic data flows and intelligence operations. In conclusion, the implementation of the EO signifies a pivotal step in transatlantic data governance, aiming to bridge regulatory disparities between the EU and the U.S. while upholding high standards of data protection and privacy. The ongoing evaluation and refinement of adequacy decisions will be crucial in ensuring continued compliance with EU legal frameworks and maintaining trust in international data transfers.

Moreover, the purpose limitations stipulated in the executive order are broad and potentially modifiable by the President, prompting apprehensions regarding their efficacy in curbing the misuse of personal data. Despite the advancements seen in the newly instituted redress mechanism compared to earlier frameworks, there persists uncertainty surrounding its independence and effectiveness in empowering individuals to fully assert their privacy rights. The expansive nature of the purpose limitations implies they encompass a wide range of potential uses for collected data, which may evolve over time based on presidential discretion. This flexibility

introduces challenges in ensuring consistent adherence to stringent privacy protections, raising concerns about the adequacy of safeguards against misuse or unauthorized access to personal information. While the redress mechanism represents a step forward by providing a formal avenue for individuals to address grievances related to data handling by intelligence agencies, its efficacy hinges on factors such as the impartiality of oversight bodies and the accessibility of remedies offered.[49] Questions remain regarding the degree of autonomy and authority granted to these bodies, as well as their capacity to conduct thorough investigations and enforce remedial actions in cases of privacy violations. Achieving robust privacy protection requires continuous refinement and adaptation of legal frameworks to keep pace with technological advancements and evolving threats to personal data security. Strengthening the independence and effectiveness of redress mechanisms is critical to ensuring that individuals can confidently exercise their privacy rights in an increasingly interconnected and data-driven world.

What is worth saying is that it will be very interesting to see if EO and DPF may become either Privacy Shield II or Schrems III. Considering historical development and native U.S. patriotism, I would bet on the latter.

References

Chander, A. (2023). Privacy and/or Trade. The University of Chicago Law review, 90(1), pp 49-136.
Determan, L. (2023). The EU – US data privacy framework and the impact on companies in the EEA and USA compared to other international data transfer mechanisms. Journal of Data protection & Privacy, 6(2), pp 120-134.
Dimović Z. (2023). Privacy and Data Protection Concerns in the Regulatory Framework of Slovenian Energy Law. LeXonomica, 15(1), pp. 53-76.
Gerke, S. (2023). Privacy Shield 2.0: A New Trans-Atlantic Data Privacy Framework Privacy Shield 2.0: A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States. Cordozo Law Review, 45(2), pp. 351-403.
Halabi, S.F. (2022). Executive authority under the U.S. constitution to enter a pandemic treaty or other international agreement. Harward international law journal online, 63/2022, pp 1-23.
Jackson, V.C. (2015). Constitutional Law in an age of Proportionality. The Yale law journal, pp. 3094-3193.
Joel, A. (2023). Necessity, proportionality and Executive order 14086. Digital commons at American University Washington College of law, pp. 1-31.
Lindsay, D. (2018). The role of proportionality in accessing Trans-Atlantic flows of personal data. Cambridge University press, pp 49-84.

[49] "European Parliament, Think Tank, Briefing research, The future of data protection and privacy: How the European Parliament is responding to citizens' expectations, 27-04-2022" Accessed June 24, 2024. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)729396

Marconi, F. (2023). The EU–US Data Protection Framework: Balancing Economic, Security and Privacy Considerations. Istituto Affari Internazionali commentaries 23(46), pp 1-7.
McCabe, D. 2022. U.S. and European leaders reach deal on trans-Atlantic data privacy. The New York Times.
Mildebrath, H.A. (2022). Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086. European Parliamentary Research Service. PE 739.261, pp 1-12.
Propp, K. (2023). More than adequate: New directions in International Data Transfer Governance. Atlantic council, Europe Center, pp 1-18.
Reinfeld, Y. (2024). The European Union as a normative power: The role of the CJEU. Routhledge, New York.
Rubinstein, I., (2022). EU Privacy Law and U.S. Surveillance: Solving the Problem of Transatlantic Data Transfers. Horizons: Journal of International Relations and Sustainable Development, 20(1), pp 58-69.
Schwartz, P.M. (2013). The EU-U.S. privacy collision: A turn to institutes and procedures. Harward Law Review, 126(7), pp 1966-2009.
Zemer, L. (2021). European Union law as foreign law. Vanderbilt Journal of Transnational law, 54(3), pp 677-692.