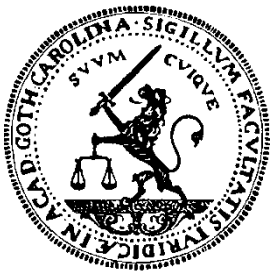

FACULTY OF LAW

LUND UNIVERSITY

Dilara Gurbanova

Evolving Data Privacy Landscapes: From Safe Harbor to the 2023 Framework – Analyzing Progress, Challenges, and the Horizon for Transatlantic Data Transfers

JAEM03 Master Thesis

European Business Law

30 higher education credits

Supervisor: Jaakko Salminen

Term of graduation: Spring, 2024

Table of contents

Abbreviations

ADR - Alternative Dispute Resolution

BCR - Binding Corporate Rules

CFR - Charter of Fundamental Rights of the European Union

CJEU - Court of Justice of the European Union

CLPO - Civil Liberties Protection Officer

DoC - Department of Commerce

DPA - Data Protection Authority

DPF - Data Privacy Framework

DPRC - Data Protection Review Court

EDPB - European Data Protection Board

EO - Executive Order

EU - European Union

FISA - Foreign Intelligence Surveillance Act

FISC - Foreign Intelligence Surveillance Court

FISCR - Foreign Intelligence Surveillance Court of Review

FTC - Federal Trade Commission

GDPR - General Data Protection Regulation

LIBE - Committee on Civil Liberties, Justice and Home Affairs (European Parliament)

OECD - Organisation for Economic Co-operation and Development

PCLOB - Privacy and Civil Liberties Oversight Board

SCC - Standard Contractual Clauses

US - United States

1. Introduction

In the dynamic realm of international data transfers, the intersection of privacy, technology, and transatlantic commerce has emerged as a critical area of legal, societal, and economic interest. The evolution of data privacy frameworks, particularly between the European Union and the United States, reflects a nuanced journey towards achieving a delicate balance between safeguarding personal data and facilitating the unfettered flow of information crucial for the digital economy. This thesis, titled 'Evolving Data Privacy Landscapes: From Safe Harbor to the 2023 Framework – Analyzing Progress, Challenges, and the Horizon for Transatlantic Data Transfers,' embarks on a comprehensive exploration of this journey, dissecting the intricate layers of legal frameworks, societal implications, and the practical realities of implementing stable data protection measures in an era of unprecedented digital interconnectedness.

The primary aim of this thesis is to conduct a thorough analysis and assessment of today's Data Privacy Framework (DPF), using a detailed examination of its developments as a means to this end. By dissecting the DPF section by section and comparing these with its predecessors, this approach not only reveals the changes but also facilitates a deep understanding of the current framework's structure and efficacy. This rigorous analysis is crucial for evaluating the effectiveness of the DPF, predicting future trends, and comprehending the broader implications. Through this lens, the research also explores the primary legal, societal, and economic challenges associated with transatlantic data transfers, highlights the impact of pivotal legal decisions by the Court of Justice of the European Union, and assesses the practical implementation of the DPF.

The core of this exploration delves into the succession of data transfer mechanisms—beginning with the Safe Harbor agreement, transitioning through the Privacy Shield, and culminating in the establishment of the Data Privacy Framework in 2023 (DPF). Each framework is scrutinized for its approach to bridging the divergent privacy philosophies between the EU, with its stringent General Data Protection Regulation, and the U.S., with its sector-specific and flexible privacy ethos. The analysis highlights the pivotal role of the Court of Justice of the European Union in shaping these frameworks through landmark decisions in the Schrems I and Schrems II cases, which stressed fundamental inadequacies in the U.S.'s data protection measures, particularly in the context of surveillance practices. Then I examined the DPF in a detailed manner, especially analysing the redress mechanisms, which underwent the biggest changes and improvements.

The path forward is not without challenges. Potential areas of future dispute and legal scrutiny are identified, including residual concerns over surveillance, the effectiveness of redress mechanisms, and the practical implementation of onward transfer provisions. The thesis posits that addressing

these challenges proactively is key to the DPF's ability to endure future legal challenges and to provide a stable and secure framework for transatlantic data transfers. In synthesizing these elements, the thesis presents a comparative analysis that contextualizes the evolution from Safe Harbor through Privacy Shield to the DPF, highlighting the progression towards enhanced data protection standards. This analysis not only addresses the criticisms and legal challenges that precipitated the demise of its predecessors but also sets forth a vision for the future of transatlantic data privacy cooperation.

The thesis lays the groundwork for a deep dive into the complexities of transatlantic data privacy frameworks, setting the stage for a nuanced discussion that traverses legal frameworks, societal expectations, and the technological realities shaping the future of data protection. Through this lens, the thesis aims to contribute to the ongoing discourse on privacy and data protection, offering insights into the challenges and opportunities that lie ahead in the quest for a harmonious transatlantic data transfer mechanism.

2. Methodology and Materials

This thesis adopts a multidimensional approach to examine the evolving landscape of transatlantic data privacy frameworks, particularly from the Safe Harbor agreement to the recently implemented 2023 Data Privacy Framework (DPF). To ensure a comprehensive analysis, this study utilizes a blend of doctrinal (black-letter), comparative legal, and historical legal methodologies.

Doctrinal (Black-letter) Method

The doctrinal method forms the foundation of this research, involving a detailed examination of legal texts to extract and analyze statutory provisions and judicial opinions. This method facilitated a thorough understanding of the legal principles underlying the Safe Harbor, Privacy Shield, and the 2023 DPF. The research focused on dissecting these frameworks to assess their adequacy in protecting personal data transferred from the EU to the US.

Comparative Legal Method

Using the comparative legal method, this study contrasts the European Union's and the United States' approaches to data privacy. This comparison is critical in understanding the shifts in policy and practice that led from the Safe Harbor to the 2023 DPF. The method helped in identifying the changes in each framework, assessing improvements, and highlighting persistent challenges that could lead to future legal disputes such as a potential Schrems III case.

Historical Legal Method

The historical legal method was employed to trace the evolution of transatlantic data transfer policies and the impact of landmark decisions such as Schrems I and II. This approach provided context to the developments in data privacy laws and the socio-political factors influencing these changes over time.

Case Law Analysis

Significant court cases, including Schrems I and II, were analyzed to understand their implications on the legal frameworks governing data privacy. These cases were pivotal in shaping the current data privacy norms and were thus studied in-depth to ascertain their influence on both the structure and the content of subsequent frameworks.

Use of ChatGPT

Throughout the drafting process, ChatGPT was employed as a supplementary tool to refine the academic quality of the thesis. After formulating initial drafts, sentences that seemed overly

simplistic or grammatically uncertain were revised using ChatGPT to correct English language errors and enhance the academic tone.

Sources

The bibliography includes carefully chosen laws, academic papers, court cases, and online documents. Each source was chosen to provide a deep dive into the legal, historical, and policy contexts of data privacy issues. Prominent sources include foundational EU regulations like GDPR, decisions such as the EU-US Privacy Shield, and significant case law like Schrems I and II. Scholarly contributions from experts, alongside opinions from the European Data Protection Board and reports from the European Parliament, have been instrumental in framing the narrative of this thesis.

By integrating these methodologies and tools, the thesis aims to offer a balanced and nuanced analysis of the progress, challenges, and the horizon for transatlantic data transfers under the evolving data privacy frameworks.

3. Overview and Legal Framework

The global digital economy relies heavily on the seamless flow of data across borders. However, this necessitates strong data protection frameworks to safeguard personal data outside the EU's borders. The Data Protection Directive[1] and the General Data Protection Regulation[2] represent key legislative milestones in the EU's approach to regulating these data transfers.

The DPD laid the initial groundwork for data transfer regulations, pointing out the need to ensure an adequate level of protection for personal data transferred to third countries. The GDPR, which replaced the DPD, introduced more stringent requirements for data transfers, reflecting the EU's commitment to high data protection standards.

The GDPR aims to ensure the protection of individuals with respect to the processing of personal data and to facilitate the free movement of such data. Notably, personal data under the GDPR is broadly defined to include any information related to an identifiable individual, encompassing a wide range of identifiers such as names and location data.[3]

This regulatory framework is built upon seven foundational principles, inspired by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data from 1980. These principles form the bedrock of the GDPR's approach to data protection, pointing out the importance of handling personal data with integrity and transparency.[4] Furthermore, the GDPR establishes clear provisions for the transfer of personal data to third countries, aiming to ensure that such transfers do not compromise the level of protection afforded to individuals under the GDPR.[5]

Article 44 of the GDPR sets forth the overarching requirement that any transfer of personal data to a third country must occur under conditions that ensure the protection of the data subject's rights and freedoms. Chapter V of the GDPR delineates the mechanisms and conditions under which such transfers are permissible, stressing the need to maintain the level of protection guaranteed by the GDPR.[6] This legislative intent is reflective of the EU's broader objective to foster the free flow of information while safeguarding personal data, as highlighted in scholarly commentary.[7]

---

[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 [1995] OJ L281.
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119
[3] Regulation (EU) 2016/679, Article 4
[4] Regulation (EU) 2016/679, Article 5
[5] Regulation (EU) 2016/679, Recital 6)
[6] General Data Protection Regulation, Article 44
[7] Christopher Kuner, 'Art. 44' in GDPR Commentary

The legislation delineates several mechanisms for transferring personal data to third countries, including adequacy decisions, appropriate safeguards such as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs), and derogations for specific situations. Notably, adequacy decisions by the European Commission certify that a third country offers a level of data protection comparable to that within the EU, thereby facilitating data transfers without the need for additional safeguards.[8] In instances where an adequacy decision is not in place, entities must implement appropriate safeguards or rely on specific derogations to ensure the protection of personal data during its transfer to third countries.[9]

This comprehensive approach reflects the GDPR's ambition to establish a reliable framework for data protection that not only addresses the challenges of data processing within the EU but also the complexities associated with transborder data flows. Through its detailed provisions on data transfers, the GDPR seeks to balance the need for data mobility in a globalized economy with the imperative to protect personal data against potential risks arising from varying legal standards in third countries.

3.1. The United States Model

In contrast to the European Union's approach, the United States has traditionally favored a more flexible model, prioritizing the economic benefits of e-commerce and data flows. Regulation was seen as potentially hampering the economic prospects of corporations benefiting from widespread internet use. This perspective led to a preference for self-regulation over comprehensive legislative measures, with an intrinsic belief in the capacity of companies to implement meaningful privacy regimes on their own.[10]

This approach was supported publicly by the U.S. government, endorsing the private sector's initiative to incorporate privacy safeguards.[11] However, this "religion of self-regulation" has been

[8] Regulation (EU) 2016/679, Article 45
[9] Regulation (EU) 2016/679, Articles 46 and 49
[10] Henry Farrell, 'Negotiating Privacy Across Arenas: The EU-U.S. "Safe Harbor" Discussions' in Adrienne Héritier ed, Common Goods: Reinventing European and International Governance (2002) 101, 105-126.
[11]The White House, A Framework for Global Electronic Commerce https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html last updated 1997

criticized for its effectiveness in protecting privacy, particularly in an era where data breaches and privacy concerns have become rampant.[12]

To evaluate whether a non-EU country offers an adequate level of protection under GDPR Article 45, it's crucial to understand its legal framework concerning privacy and data protection. The United States, home to the majority of leading digital corporations, plays a pivotal role in EU-US data transfers, crucial for their combined $7.1 trillion[13] economic value. Unlike the EU, the US approaches privacy through a patchwork of state and federal laws without a unified privacy definition, leading to a reactive rather than proactive legal stance on privacy and data protection. This reflects broader philosophical differences, with the US prioritizing a more laissez-faire attitude towards business and a higher value on freedom of expression over privacy, contrasting with Europe's focus on individual privacy rights.[14]

In the US, privacy rights are less explicit at the federal level, with no direct mention in the Constitution or Amendments. It was not until the Griswold v. Connecticut case[15] in 1965 that the Supreme Court recognized privacy rights inferred from the Bill of Rights, highlighting a fragmented approach to privacy. Despite this, the US has developed a series of statutes and common law doctrines that form a reactive patchwork of privacy laws, lacking a coherent federal privacy law or a clear constitutional right to data protection. The situation becomes even more complex with the statutory laws' diverse interpretations of "privacy" and the absence of a unified approach to data protection.[16]

Regarding government data protection regimes, the US has sector-specific laws like the Privacy Act of 1974 and the Foreign Intelligence Surveillance Act, which governs the use of data by federal agencies and the surveillance practices respectively. These laws illustrate the fragmented and sector-oriented approach to data protection in the US, further complicated by various exemptions and limitations. The Privacy Act's applicability primarily to US citizens and residents highlights a significant limitation for non-US individuals concerning data protection rights in the US.[17]

---

[12] Paul M. Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vand. L. Rev. 1609. Joel R. Reidenberg & Francoise Gamet-Pol, 'The Fundamental Role of Privacy and Confidence in the Network' (1995) 30 Wake Forest L. Rev. 105, 113-14.

[13] The White House, 'FACT SHEET: European Commission Announce Trans-Atlantic Data Privacy Framework' (25 March 2022) https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ accessed 04 April 2024

[14] Steven C Bennett, 'The "Right to be Forgotten": Reconciling EU and US Perspectives' (2012) 30(1) Berkeley Journal of International Law 161, 169.

[15] Griswold v Connecticut (1965) 381 US 479.

[16] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193.

[17] United States Department of Justice, 'Overview of the Privacy Act of 1974' (Office of Privacy and Civil Liberties, 2015) 4.

The judicial response to privacy and data protection issues, such as in the Griswold case and subsequent rulings, illustrates the US's evolving but still fragmented legal landscape regarding these rights. The US legal system's approach to privacy and data protection, characterized by its sector-specific legislation and the significant role of judicial interpretation, contrasts with the more comprehensive and individual-centric frameworks found in the EU.

Recent developments, however, indicate a shift in the U.S. stance towards privacy, with high-profile cases such as Google CEO Sundar Pichai declaring privacy a human right during a congressional hearing.[18] Additionally, the California Consumer Privacy Act has introduced new rights for California residents, reflecting a more nuanced approach to privacy that could signify a departure from the previously predominant model of self-regulation.

3.2. Adequacy Decisions: Criteria and Process

Adequacy decisions are a pivotal component of the EU's data transfer framework, allowing for the free flow of data to countries deemed to have equivalent data protection standards. The DPD first introduced this concept, outlining the criteria for assessing a third country's level of protection.[19] The GDPR expanded these criteria significantly, including considerations related to the rule of law, human rights, and access to personal data by public authorities.[20]

The process for adopting adequacy decisions involves a comprehensive assessment by the European Commission, with input from various stakeholders, including the European Data Protection Board (EDPB) and Member States. This process highlights the procedural differences between the DPD and GDPR, with the latter providing a more detailed and rigorous framework for these assessments.

3.3. Impact on Data Transfers and Protection Level

The adequacy decision mechanism facilitates data transfers by eliminating the need for additional safeguards. Under the GDPR, the criteria for adequacy assessments have been broadened, requiring a comprehensive review of the third country's data protection landscape.[21] This

[18] Tony Romm, 'Amazon, Apple, Facebook and Google Grilled on Capitol Hill over Their Market Power' *The Washington Post* (29 July 2020) https://www.washingtonpost.com/technology/2020/07/29/apple-google-facebook-amazon-congress-hearing/
[19] Directive 95/46/EC, art 25(2)
[20] Regulation (EU) 2016/679, art 45(2)(a)
[21] Regulation (EU) 2016/679, art 45

mechanism ensures that personal data transferred to these countries enjoy a level of protection essentially equivalent to that guaranteed within the EU, significantly impacting the protection level of personal data.

3.4. Safeguards for Data Transfers without Adequacy Decisions

In the absence of an adequacy decision, the GDPR provides mechanisms such as Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCR) to ensure the protection of personal data transferred to third countries.[22] These instruments ensure the necessary safeguards when an adequacy decision is not applicable. SCCs, approved by the European Commission, provide minimum safeguards and are streamlined for convenient use, ensuring GDPR compliance. BCRs, used for transfers within corporate groups, must be authorized by a competent supervisory authority and ensure equal data protection across all entities. Codes of conduct[23], developed by industry groups, must be legally binding and enforceable, ensuring high data protection standards before third-country entities can join. Certification mechanisms promoted by supervisory authorities increase transparency and accountability, benefiting both data subjects and businesses. In cases where these safeguards are absent, derogations can be applied if the data subject is informed and consents to the transfer, ensuring compliance with GDPR requirements.[24]

[22] Regulation (EU) 2016/679, art 46
[23] EDPS Guidelines 04/2021 on Codes of Conduct as tools for transfers
[24] Regulation (EU) 2016/679, art 46

4. Historical Context and Evolution

A detailed look at the progression from Safe Harbor to Privacy Shield, and finally to the DPF

The evolution of data transfer frameworks between the European Union and the United States represents a significant journey towards achieving stronger data protection and privacy standards. This journey, marked by legal and societal changes, evolved through several stages, starting with the Safe Harbor agreement, moving through the Privacy Shield, and culminating in the adoption of the Data Privacy Framework (DPF).

4.1. Safe Harbor

Introduced in the year 2000, the Safe Harbor framework[25] was an initial attempt to bridge the gap between the EU's comprehensive approach to privacy protection and the US's sector-specific approach. It allowed US companies to self-certify compliance with privacy principles that were deemed adequate by the EU. The principles central to the framework were Notice, Choice, Onward transfer, Security, Data integrity, Access, and Enforcement. Organizations could only forward data if the third parties promised at least equivalent privacy protection.[26]

The process to join the Safe Harbor framework was based on organizations self-certifying through an annual letter to the Department of Commerce, which included administrative details and a description of the organization's privacy policy and independent recourse mechanisms.[27] This approach was deliberately designed to leave enforcement of the Safe Harbor principles mostly to the private sector, as indicated by official government guidelines.[28] Furthermore, the framework assigned dispute resolution to various third-party mechanisms, without standardization, and lacked initial oversight, leaving the enforcement of EU subjects' data protection rights predominantly to the private sector.[29]

Concerns about the effectiveness of the framework in protecting EU citizens' data from US surveillance led to criticism. The European Court of Justice (ECJ) invalidated the Safe Harbor agreement in 2015 (Case C-362/14, Maximilian Schrems v. Data Protection Commissioner)[30],

---

[25]Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215.

[26] Commission Decision 2000/520/EC, Annex I.

[27] U.S. Department of Commerce, 'Safe Harbor Overview' (2002) [accessed 13 April 2024] https://web.archive.org/web/20020601115555/www.export.gov/safeharbor/sh_overview.html

[28] U.S. Department of Commerce, 'Safe Harbor Overview' (2002) [accessed 13 April 2024] https://web.archive.org/web/20020601115555/www.export.gov/safeharbor/sh_overview.html

[29] U.S. Department of Commerce, 'Safe Harbor Overview' (2002) [accessed 13 April 2024] https://web.archive.org/web/20020601115555/www.export.gov/safeharbor/sh_overview.html

[30] Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

citing inadequate protection against US intelligence agencies' access to data. CJEU invalidated the Safe Harbor agreement, not on the basis of its principles being inherently inadequate, but because the European Commission had not fully evaluated the US's overall legal framework regarding public authorities' access to data.

This judicial decision pointed out two essential points. Firstly, the adequacy of protection by a third country must ensure a level of fundamental rights and freedoms that is "essentially equivalent" to that guaranteed within the EU. Secondly, it affirmed that DPAs within EU member states have the authority to examine the lawfulness of data transfers to a third country, despite an existing European Commission adequacy decision.[31]

The CJEU's judgment rendered the Safe Harbor framework invalid, plunging transatlantic data transfers into legal uncertainty. It necessitated the exploration of alternative mechanisms such as the EU Model Contracts and Binding Corporate Rules for legal data transfers. Nonetheless, the judgment also raised profound questions regarding the feasibility of any data transfer mechanism under scrutiny of US law, particularly concerning national security and surveillance practices.

The invalidation of Safe Harbor thus represents a critical juncture in EU-US data protection relations, highlighting the challenges of reconciling the EU's stringent data privacy standards with the US's more lenient approach, especially in the context of national security. This development has propelled efforts to negotiate a new framework for transatlantic data transfers, aiming to ensure a stable legal basis for the crucial flow of information that underpins the EU-US economic relationship.

4.2. Privacy Shield

Following the invalidation of the Safe Harbor framework, the Privacy Shield agreement[32] emerged as its successor, aiming to address the legal and privacy concerns that led to Safe Harbor's demise. The Privacy Shield was designed to provide a more robust framework for the transfer of personal data from the European Union to the United States, reflecting the continued economic interdependence between these two major economies. Similar to its predecessor, the Privacy Shield was predicated on the need for non-EU countries to offer an "adequate" level of data protection to receive personal data from the EU. The Privacy Shield sought to establish a voluntary mechanism

[31] Neal Cohen, 'The Privacy Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework' (2015) 1 Eur Data Prot L Rev 240)

[32] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield [2016] OJ L207

where US companies could commit to higher standards of data protection, in line with EU expectations, thereby being recognized as providing "adequate" protection.

Several pivotal modifications were implemented to enhance data protection standards. These included the introduction of more solid security protocols, which were now tailored according to the type of data handled and a comprehensive risk evaluation, deviating from the prior approach that merely required reasonable measures.[33] The scope for accessing personal data was broadened, simultaneously introducing a principle of data minimization concerning the duration of data retention. Specifically, entities were permitted to hold onto data solely for periods that fulfilled a processing objective,[34] moving away from the previous indefinite retention model seen under the Safe Harbor framework. In scenarios involving data being passed to a third party, the recipient was obligated to ensure protection parity with the originating party,[35] and individuals were granted the option to refuse their data being shared with third parties, albeit with some exceptions. Additionally, mechanisms for seeking recourse were revised to be cost-free, a significant shift from the previous requirement for such mechanisms to be simply accessible and economically feasible.

Privacy Shield Principles: The Privacy Shield framework was structured around several key principles similar to those of Safe Harbor, including Notice, Choice, Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Enforcement and Liability. These principles were intended to ensure that participating organizations provide clear information about their data processing practices, offer individuals choices regarding the use and disclosure of their personal data, ensure the secure transfer of data to third parties, maintain the integrity and purpose of personal data, and provide access to individuals to their own data. A significant focus was placed on stronger enforcement measures and greater accountability for data processors, addressing one of the major criticisms of the Safe Harbor framework.[36]

Onward Transfer Requirements: Like its predecessor, the Privacy Shield required that any onward transfer of data from a Privacy Shield-certified organization to a third party had to ensure that the third party provided at least the same level of privacy protection as required by the Privacy Shield principles. This requirement was aimed at creating a continuous protection chain for personal data transferred from the EU to the U.S. [37]

[33] Commission Implementing Decision (EU) 2016/1250, rec 24
[34] Commission Implementing Decision (EU) 2016/1250, Annex II, II.5(b)
[35] Commission Implementing Decision (EU) 2016/1250, rec 28
[36] EU-US Privacy Shield Framework, Privacy Principles, sec 2.1.
[37] EU-US Privacy Shield Framework, Principles, sec III 'Onward Transfers'

Self-certification and Annual Re-certification: Entry into the Privacy Shield framework, similar to Safe Harbor, was based on a self-certification process. Organizations wishing to participate in the Privacy Shield had to annually certify with the U.S. Department of Commerce that they adhered to the Privacy Shield principles. This process included providing a detailed privacy policy that complied with the principles, publicly committing to comply with them, and implementing an independent recourse mechanism for resolving complaints.[38]

Private Sector Enforcement and Dispute Resolution: The Privacy Shield framework sought to strengthen the enforcement of its principles by mandating more rigorous monitoring and compliance verification by the U.S. Department of Commerce and the Federal Trade Commission (FTC). It introduced a range of dispute resolution mechanisms, including free access to alternative dispute resolution (ADR) for EU individuals, and the possibility of binding arbitration as a last resort. Furthermore, the Privacy Shield established a greater role for European Data Protection Authorities (DPAs) in handling complaints and disputes, aiming to improve the protection of EU individuals' rights and ensure effective legal remedies.[39]

Enhanced Oversight and Cooperation: Recognizing the shortcomings in oversight within the Safe Harbor framework, the Privacy Shield introduced mechanisms for more active monitoring and review of compliance by the U.S. Department of Commerce. It also established a framework for cooperation between the Department of Commerce, the FTC, and European DPAs to ensure that complaints and issues are addressed more effectively and efficiently. [40]

In summary, while the Privacy Shield built upon the foundational principles of the Safe Harbor framework, it aimed to address the critical issues identified by the ECJ, particularly in terms of enforcement, accountability, and the protection of EU individuals' rights.

However, the Privacy Shield, like the Safe Harbor agreement before it, faced significant challenges. Concerns persisted regarding the extent of US intelligence agencies' surveillance activities and whether the Privacy Shield adequately safeguarded EU citizens' data against such practices. The framework's efficacy was ultimately challenged in the Court of Justice of the European Union in the case known as Schrems II. Here, the CJEU scrutinized the Privacy Shield's ability to ensure that the level of protection for personal data was "essentially equivalent" to that within the EU, as mandated by EU data protection laws.

[38] EU-US Privacy Shield Framework, Annex I 'Self-Certification
[39] EU-US Privacy Shield Framework, sec IV 'Dispute Resolution and Enforcement
[40] EU-US Privacy Shield Framework, Annex II 'Cooperation with European Data Protection Authorities.

In its landmark decision Schrems II[41], the CJEU invalidated the Privacy Shield framework, determining that it failed to adequately address the US's surveillance practices. The judgment reaffirmed the principle that an adequate level of protection must essentially mirror the protection guaranteed within the EU, stressing the importance of safeguarding fundamental rights and freedoms. Moreover, the ruling reinforced the authority of Data Protection Authorities (DPAs) within EU member states to scrutinize data transfers to the US, irrespective of any adequacy decision by the European Commission.

The invalidation of the Privacy Shield placed transatlantic data transfers under renewed legal uncertainty, prompting stakeholders to seek alternative legal mechanisms for such transfers, including the use of Standard Contractual Clauses and Binding Corporate Rules. The CJEU's decision highlighted the ongoing concerns regarding the compatibility of US law, particularly surveillance laws, with EU data protection standards.

The Schrems II ruling thus marked another critical moment in the evolution of EU-US data protection relations, spotlighting the ongoing challenges of aligning US data privacy practices with the EU's stringent data protection regime. This development has accelerated discussions and negotiations aimed at crafting a new and durable framework for data transfers across the Atlantic, accentuating the necessity of finding a balanced and legally sound solution to facilitate the vital economic relationship between the EU and the US.

Following the Schrems II judgment, the quest for a stable transatlantic data transfer framework became more pressing. The Court of Justice of the European Union pointed out the significant disparities between U.S. and EU approaches to privacy and data protection, notably in the context of government surveillance activities. This discrepancy has propelled efforts to reconcile these differences to ensure a secure and legally compliant data transfer environment.

In particular, the Schrems II decision stressed the necessity for any data transfer mechanism to provide protections equivalent to those afforded within the EU, as mandated by the Charter of Fundamental Rights of the European Union and the General Data Protection Regulation. The ruling criticized the U.S. surveillance programs, including those under Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, for their broad data collection practices and the insufficient judicial oversight and remedies available to individuals[42]. These concerns

[41] Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems [2020] ECLI:EU:C:2020:559

[42] Schrems II (n 43) paras 179, 181, 183.

highlighted the need for reforms in U.S. law to align with the EU's stringent data protection standards.

The CJEU's insistence on proportionality, necessity, and the presence of adequate safeguards for personal data underlines the European commitment to ensuring a high level of protection for individuals' data. This approach demands clear and precise regulations on the scope of data collection and use, particularly by government authorities, to prevent excessive and unjustified intrusions into personal privacy.[43]

The aftermath of the Schrems II ruling has been a period of reflection and action for both the EU and the U.S. to find a pathway towards compliance and mutual recognition of data protection standards. The emphasis has been on developing a new framework that addresses the CJEU's concerns, particularly around the issues of surveillance, data subject rights, and legal recourse. This endeavor aims not only to restore confidence in transatlantic data flows but also to support the continued economic partnership between the EU and the U.S.

The dialogue and negotiations that have ensued seek to establish a mechanism that respects the fundamental rights of EU citizens while acknowledging the security interests of the U.S. Such a solution would require adjustments in U.S. surveillance practices, enhanced transparency, and the establishment of effective judicial redress options for EU citizens, addressing the gap identified in the Schrems II decision regarding the principle of equality and access to justice. This process accentuates the dynamic nature of international data protection law and the ongoing efforts to align disparate legal systems in the digital age.

As this dialogue progresses, the implications for both large multinational corporations and smaller entities are profound. While larger organizations may navigate these changes with relative ease, the impact on smaller businesses highlights the need for scalable and feasible compliance solutions. This consideration is crucial in ensuring that the economic benefits of transatlantic data flows are accessible to all sectors of the economy, not just the most resource-rich players.

With the adoption of the new adequacy decision, a significant stride has been made towards addressing the legal and privacy concerns highlighted by the Schrems II ruling. This development marks a pivotal moment in EU-U.S. data protection relations, offering a renewed legal basis for transatlantic data transfers. The decision is crafted to ensure that the stringent EU standards for data protection are met, incorporating enhanced safeguards and mechanisms for oversight to address the issues of surveillance and data subject rights previously identified by the CJEU. For

[43] Schrems II (n 43) para 177; Opinion 1/15, ECLI:EU:C:2017:592, paras 140-141 (26 July 2017).

businesses, especially smaller enterprises, this creates a more predictable and secure legal environment for data flows, potentially easing the compliance burden and facilitating smoother international operations. This new framework points out a collaborative effort between the EU and U.S. to uphold the fundamental right to privacy while supporting economic relations and technological cooperation.

4.3. Evaluating Reforms: The Path Towards a Resilient Data Transfer Framework

The Schrems I and II cases highlight significant concerns over the transfer of EU citizens' personal data to the United States, revealing serious implications for national security and individual rights. The Court of Justice of the European Union (CJEU) found issues with the U.S.'s handling of data, leading to the invalidation of both the Safe Harbor and Privacy Shield agreements. The crux of the matter revolves around two main issues:

First, there was a clear failure to adhere to the principle of proportionality; the U.S. data access and processing activities extended well beyond what was deemed necessary for national security, undermining the essence of privacy rights.[44] In Schrems I, it was determined that the U.S. authorities' broad access to electronic communications was incompatible with the data's original transfer purposes, violating privacy rights as guaranteed by the Charter.[45] Similarly, Schrems II criticized the lack of minimal safeguards under U.S. surveillance programs, marking them as disproportionate.[46]

Second, the absence of legal recourse for individuals to access, rectify, or erase their data was pointed out. This lack of judicial remedy violates the fundamental right to effective judicial protection.[47] Schrems II further criticized the inadequacy of the Privacy Shield's ombudsperson mechanism, highlighting its failure to provide equivalent guarantees as required by the Charter.[48]

These cases highlight the need for significant reforms in U.S. laws and practices to ensure any future data protection agreement can withstand scrutiny by the CJEU, stressing the importance of both proportionality in data processing for national security and the availability of legal remedies for individuals.

---

[44] Charter of Fundamental Rights of the European Union, art 52(1)
[45] Case C-362/14, Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650, paras 90, 94
[46] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559, para 184
[47] Case C-362/14, Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650, para 95
[48] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559, para 197.

5. Data Privacy Framework[49]

The invalidation of the Privacy Shield necessitated a new approach, leading to the negotiation of the EU-US Data Privacy Framework. The DPF was designed to address the CJEU's concerns by implementing substantial changes in US law and practice. The new framework was meant to:

- Bolster the protections for privacy and civil rights concerning the signal intelligence operations in the United States;
- Introduce a fresh method for addressing grievances, featuring an autonomous and decisive authority; and
- Improve the already stringent and multi-level scrutiny of signal intelligence operations.

These goals specifically tackled the concerns highlighted in the Schrems II decision.[50]

The US Department of Commerce (DOT) expressed a longstanding commitment to enforcing these data protection frameworks, starting over two decades ago with Safe Harbor and reiterated for the Privacy Shield and now the DPF.[51] This commitment underscores a continuous effort to enhance privacy protections in transatlantic data transfers.

The DPF represents a step forward in the approach to data privacy, incorporating elements that address some of the CJEU's criticisms. The negotiations followed the Schrems II ruling, focusing on ensuring that the new framework would meet the standards set by the CJEU for data protection.[52] This included the adoption of Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities' and the establishment of a Data Protection Review Court, indicating a shift in the US approach to surveillance and privacy protections.[53]

Despite this progress, the fundamental structure and principles remain largely unchanged from the Privacy Shield, with about 90% of the text staying the same. This continuity, especially considering the CJEU's concerns in Schrems II, may undermine the framework's effectiveness.[54]

---

[49] Commission Implementing Decision (EU) 2023/4745 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework [2023] OJ L207.

[50] Andrej Savin, 'EU-US Data Privacy Framework – The New Framework for Transatlantic Data Transfers' (2023) 4 EuCML 159

[51] Commission Implementing Decision (EU) 2023/4745, Annex V.

[52] Commission Implementing Decision (EU) 2023/4745, Introduction, paras 5, 6.

[53] Commission Implementing Decision (EU) 2023/4745, Introduction, para 6

[54] Galehr, Stella, Transatlantic Data Transfers under the GDPR: Developments and Outlook (Zurich Open Repository and Archive, University of Zurich 2023) https://doi.org/10.5167/uzh-252334 accessed [16.05.2024]

The introduction of the DPF underscores the shared commitment between the US and EU to enhance privacy protection, acknowledging the different approaches taken by each party. This mutual recognition of the importance of transatlantic data flows, coupled with a commitment to stronger privacy protections, is foundational to the DPF's development.[55] Moreover, the framework is presented as a basis for a new adequacy decision by the European Commission, highlighting its potential to align with the EU's data protection standards more closely than its predecessors.[56]

The change from Safe Harbor to Privacy Shield, and then to the DPF, shows a shift towards stronger data protection. This change was influenced by court decisions, society's call for privacy, and detailed discussions across the Atlantic about balancing security with personal rights. The DPF represents the latest effort to address these complex issues, aiming to establish a durable foundation for future data transfers that respects both the privacy of individuals and the security interests of nations.

5.1. Institutional Dynamics in the EU's Data Protection Framework: The EDPB, European Parliament, and Committee Deliberations

Delving into the intricacies of the European Union's data protection and transfer framework requires an examination of the pivotal roles of its key stakeholders. This exploration is not just about understanding their opinions and actions but also about appreciating the depth of their impact on adequacy decisions which are central to the EU’s approach to ensuring high levels of data protection for cross-border data flows that lack such decisions.

The European Data Protection Board (EDPB) thoroughly examined the draft adequacy decision, released on December 13, 2022, and by February 28, 2023, provided its comprehensive feedback. The EDPB acknowledged the positive strides made by incorporating principles of necessity and proportionality as outlined in Executive Order 14086. It also welcomed the establishment of a novel complaints handling system. However, it aired significant concerns regarding aspects such as individual rights, the specifics of data transfers, exemptions, the practice of bulk data collection, and the actual effectiveness of the redress mechanism. Moreover, the EDPB advocated for the

[55] Commission Implementing Decision (EU) 2023/4745, Annex I 'Overview'
[56] Commission Implementing Decision (EU) 2023/4745, Annex II 'Introduction'

decision’s enforcement to hinge on the U.S. intelligence agencies' adherence to updated guidelines as per Executive Order 14086, alongside a Commission's reassessment of these policies. It underscored the issues with bulk data collection that lacked prior independent authorization and stressed the importance of enhancing the redress mechanism, including the necessity for an independent review post-collection to align with recent European Court of Human Rights jurisprudence.[57]

Parallel to the EDPB’s deliberations, the European Parliament, through its Committee on Civil Liberties, Justice, and Home Affairs (LIBE), undertook a critical assessment of the EU-US Data Privacy Framework. In its Draft Motion for a Resolution, issued on February 14, the committee voiced its apprehension about the framework’s capacity to ensure a protection level equivalent to that of EU norms and the Charter of Fundamental Rights. It was particularly concerned about the expansive interpretation of proportionality in intelligence activities, the permission for bulk data collection, and the authority of the president to alter national security objectives without any public accountability. Furthermore, the Data Protection Review Court’s opaque and executive-aligned decision-making process, coupled with inadequate representation for complainants, was criticized for undermining the rights of individuals to access, correct, and challenge decisions about their data. Despite adopting the draft motion with amendments, indicating a perceived improvement in the framework, the Committee and later the European Parliament remained skeptical of its sufficiency for ensuring the safe transfer of personal data, urging for a postponement of the adequacy decision until full compliance with the EDPB’s recommendations was achieved.[58]

While the insights from the EDPB and the European Parliament don’t dictate policy directly, they significantly influence the European Commission’s stance on EU-US data transfer agreements. A pivotal moment came on July 6, 2023, when a strong majority of EU countries endorsed a revised version of the data transfer proposal, showcasing a nuanced interplay of interests and concerns within the EU. Despite no major modifications being made to the underlying principles of Executive Order 14086, this endorsement signified a critical step in the ongoing transatlantic dialogue on data privacy and protection standards. The EC, thus, opted not to demand substantial

[57] European Data Protection Board, 'Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data under the EU-US Data Privacy Framework' (28 February 2023) https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf accessed 3 April 2024)

[58] European Parliament, 'Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework' (P9_TA 0204, 2023) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.pdf accessed 03 April 2024, European Parliament, 'Resolution on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework' (11 May 2023) https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1744353&t=e&l=en accessed 03 April 2024).

changes from the US, reflecting a strategic choice in navigating the complex dynamics of international data privacy standards.[59]

This collective scrutiny and feedback mechanism illustrate the European Union's rigorous approach toward safeguarding personal data in transatlantic transfers. By meticulously analyzing the draft adequacy decision, both the EDPB and the European Parliament have played a crucial role in shaping the future of EU-US data privacy relations. Their evaluations, stressing the need for a framework that upholds the principles of necessity, proportionality, and effective redress, reflect a deep commitment to protecting individual rights within the context of international data flows.

The conditional endorsement by the European Commission, contingent upon the adherence of the U.S. to certain principles and the implementation of improvements in data protection practices, reinforces the complex interplay between regulatory frameworks and international diplomacy. It highlights the EU's intent to maintain a high standard of data protection while engaging in constructive dialogue with the United States. This balancing act is indicative of the broader challenges faced in harmonizing data protection standards across jurisdictions, which requires not only rigorous assessment and critique but also a willingness to adapt and refine legal instruments in response to evolving needs and insights.

In conclusion, the EU's journey towards the new adequacy decision of 2023, marked by the intricate processes of review, feedback, and endorsement, exemplifies the union's steadfast dedication to upholding the highest standards of data protection. Through a collaborative and multi-faceted examination of the proposed EU-US Data Privacy Framework, the EU has sought to ensure that cross-border data transfers do not compromise the fundamental rights of its citizens, thereby setting a precedent for future international data protection agreements. This process, enriched by the contributions of the EDPB, the European Parliament, and the European Commission, illustrates the importance of robust institutional engagement in the formulation of policies that have far-reaching implications for privacy, security, and the transatlantic relationship at large.

[59]Davinia Brennan, 'European Commission Publishes Draft Adequacy Decision for EU-US Data Transfers' (MATHESON, 15 December 2022) https://www.matheson.com/insights/detail/european-commission-publishes-draft-adequacy-decision-for-eu-us-data-transfers accessed 3 April 2024, Rosa Barcelo, Romain Perray, David P Saunders & Simon Mortier, 'EU-US Transatlantic Data Flows Framework: EU Supervisors Shine Light at the End of the Tunnel' (MCDERMOTT WILL & EMERY, 9 March 2023 https://www.mwe.com/insights/eu-us-transatlantic-data-flows-framework-eu-supervisors-shine-light-at-the-end-of-the-tunnel accessed 3 April 2024)

5.2. Core Principles of the DPF

The EU-U.S. Data Privacy Framework (DPF) represents a development in the realm of international data transfer frameworks, particularly when viewed against its predecessors, Safe Harbor and the Privacy Shield. The core principles of the DPF have been crafted to address the increasing demand for stronger data protection and privacy standards, particularly in light of the European Union's General Data Protection Regulation. This section delves into the foundational principles of the DPF, emphasizing how it builds upon the shortcomings of its predecessors to enhance data integrity, individual choice, transparency, access to data, and the protection of sensitive data.

Data Integrity and Purpose Limitation

The evolution of data privacy frameworks from Safe Harbor to Privacy Shield, and most recently to the 2023 adequacy decision, showcases a progressive tightening and clarification of the data integrity and purpose limitation principles. Under the original Safe Harbor agreement, the requirement was relatively broad, mandating that data be "relevant" and not used in a way that is incompatible with the purposes for which it was collected.[60] However, Safe Harbor faced criticism for its lack of enforcement and ambiguity in terms of data accuracy and completeness standards. This led to the European Court of Justice's invalidation of the framework in the Schrems I case, primarily due to concerns over inadequate protections against U.S. surveillance practices.

The subsequent Privacy Shield attempted to address these deficiencies by stressing that data must be "limited to what is relevant and necessary" for processing, introducing a clearer obligation for data accuracy and purpose consistency. It also implemented more reliable oversight mechanisms, including increased rights for individuals to challenge misuse of their data.[61] Despite these improvements, the Privacy Shield still struggled with enforcement credibility and was eventually struck down in the Schrems II case. Critics argued that it did not go far enough in limiting data retention and ensuring data minimization, particularly in the context of ongoing U.S. surveillance and data access by public authorities.[62]

---

[60] U.S. Department of Commerce, 'U.S.-EU Safe Harbor Framework' (2000) https://2001-2009.state.gov/p/eur/rls/or/2000/21759.htm accessed 18 May 2024

[61] U.S. Department of Commerce, 'EU-U.S. Privacy Shield Framework' (2016) https://www.privacyshield.gov/Program-Overview accessed 18 May 2024

The new DPF introduces more stringent measures on data integrity and purpose limitation, directly addressing issues highlighted in previous frameworks. It specifies that personal information can only be retained as long as it serves the processing purpose, explicitly allowing extended retention only for well-defined secondary purposes such as public interest archiving or research, where it must still comply with all other applicable principles. This new framework makes a significant advance by enforcing the principle that data should not only be accurate and relevant but also "complete and current" to the extent necessary for its intended use. This is a clear improvement in ensuring that data protection measures are practical and directly tied to the reliability of data for its intended purposes. However, the challenge remains whether these enhanced provisions will be effectively enforced, particularly against the backdrop of U.S. legal standards on data access by security agencies, potentially still leaving gaps in protection against excessive surveillance.[63]

Choice Principle

The evolution of data privacy frameworks from Safe Harbor to Privacy Shield, and most recently to the 2023 adequacy decision, showcases a progressive tightening and clarification of the Choice principle, particularly in the handling of sensitive personal information. Initially, under Safe Harbor, the Choice principle allowed individuals to opt-out of their data being used for purposes beyond the original collection, especially direct marketing.[64] However, this provision was critiqued for its vague implementation guidelines and limited enforceability scope, particularly when addressing the transfer of sensitive data.

The subsequent Privacy Shield framework attempted to strengthen the Choice principle by mandating clear disclosure to individuals about the use of their data for purposes other than those for which it was originally collected, thereby allowing them to opt out. This framework also introduced more detailed provisions concerning sensitive data, requiring explicit consent for its use, which marked a significant improvement over Safe Harbor.[65] Nonetheless, the Privacy Shield did not fully resolve ambiguities related to the timing and ease of opting out, nor did it adequately address the mechanisms through which consent could be practically and effectively withdrawn.

The DPF further refines the Choice principle by specifying the "timing of opt-out" and expanding the definition and safeguards around sensitive information. It clearly states that individuals must

[63] Commission Implementing Decision (EU) 2023/4745, Annex I 'Data Integrity and Purpose Limitation'

[64] U.S. Department of Commerce, 'U.S.-EU Safe Harbor Framework' (2000) https://2001-2009.state.gov/p/eur/rls/or/2000/21759.htm accessed 18 May 2024

[65] U.S. Department of Commerce, 'EU-U.S. Privacy Shield Framework' (2016) https://www.privacyshield.gov/Program-Overview accessed 18 May 2024

be able to opt out of direct marketing "at any time" and sets forth stringent requirements for the processing of sensitive data. Now explicitly included are data categories such as genetic and biometric data, with a mandate that organizations must obtain affirmative express consent (opt-in) from individuals to use such sensitive information for other purposes or to disclose it to third parties.[66]

Additionally, the new framework outlines exceptions to this requirement, such as in situations involving the vital interests of a person or necessary for medical care, legal claims, or public interest reasons—similar to those found in EU law. These provisions aim to provide a consistent and predictable legal environment, enhancing protections while acknowledging practical necessities.

Moreover, enhanced security measures are required under the new framework, ensuring that sensitive data is not only processed with consent but also protected against unauthorized access and breaches, considering the nature of the data and associated risks. This requirement of explicit consent coupled with tough security measures for sensitive data processing reflects a deliberate effort to align more closely with the stringent data protection expectations of the European Union.[67]

These improvements in the Choice principle under the 2023 framework address previous criticisms by making opt-out options more accessible and binding while ensuring that sensitive data receives the highest level of protection. Nonetheless, challenges remain in terms of enforcement and the practical application of these opt-out mechanisms across different organizational contexts, especially given the potential variability in how promptly and effectively opt-out requests are processed by organizations.

Transparency

The transparency principle has undergone refinement in the 2023 adequacy decision compared to its predecessors, Safe Harbor and Privacy Shield. Under Safe Harbor, transparency was somewhat vaguely defined and primarily focused on organizations disclosing their participation in the framework. There was limited focus on detailed disclosures about data processing activities, which often left data subjects inadequately informed about the use of their personal data and the rights

[66] Commission Implementing Decision (EU) 2023/4745, Annex I Choice Principle
[67] Commission Implementing Decision (EU) 2023/4745, Annex I Choice Principle

available to them.[68] This lack of specificity contributed to the European Court of Justice's concerns in the Schrems I decision, which highlighted the overall inadequacy of the U.S. data protection measures from an EU perspective.

Privacy Shield sought to enhance transparency by requiring clearer notifications to data subjects about data collection and processing purposes. It mandated organizations to inform individuals about data disclosure to third parties and the available redress mechanisms.[69] However, criticisms persisted regarding the actual implementation of these requirements, particularly in contexts involving complex data-sharing arrangements and indirect data collection methods. Although improvements were noted, the Privacy Shield was still seen as insufficient in ensuring complete transparency, particularly concerning the mechanisms of data transfer and the specific entities involved, which eventually led to its invalidation in the Schrems II ruling.

The DPF introduces a more robust transparency framework that aligns more closely with the EU's GDPR standards. It specifies that data subjects must be clearly informed of key aspects of data processing—such as the type of data collected, the purpose of processing, and details regarding third-party disclosures—using language that is clear and conspicuous. This is a significant step forward in ensuring that data subjects are not only aware but also understand the processing activities involving their personal data. The decision also mandates the public availability of privacy policies and links to various informational resources, including a comprehensive list of organizations adhering to the DPF, and records of those removed from the framework. This enhancement addresses previous gaps by ensuring transparency both at the entry and exit points of data processing certifications, thereby fostering greater accountability and facilitating better oversight by data protection authorities and the public. [70]

Sensitive Data

The handling of sensitive data under the evolving EU-U.S. data privacy frameworks highlights significant changes and ongoing challenges. The original Safe Harbor framework provided a rudimentary basis for sensitive data, requiring affirmative consent for its processing unless certain conditions were met, such as legal or medical necessities.[71] However, it was criticized for its lack

[68] U.S. Department of Commerce, 'U.S.-EU Safe Harbor Framework' (2000) https://2001-2009.state.gov/p/eur/rls/or/2000/21759.htm accessed 18 May 2024

[69] U.S. Department of Commerce, 'EU-U.S. Privacy Shield Framework' (2016) https://www.privacyshield.gov/Program-Overview accessed 18 May 2024

[70] Commission Implementing Decision (EU) 2023/4745, Annex I, Transparency

[71] U.S. Department of Commerce, 'U.S.-EU Safe Harbor Framework' (2000) https://2001-2009.state.gov/p/eur/rls/or/2000/21759.htm accessed 18 May 2024

of explicit protections and clarity which led to ambiguities in implementation. This framework was deemed insufficient in the context of growing digital data flows and the increasing complexity of data-driven operations, particularly highlighted by the European Court of Justice's invalidation in the Schrems I decision, largely due to concerns over inadequate protection against U.S. surveillance.

The Privacy Shield sought to address these deficiencies by tightening the conditions under which sensitive data could be processed without explicit consent, but it still fell short of European standards in terms of explicit consent and the broad exemptions it allowed, such as for national security purposes.[72] Moreover, while it added more defined categories and clearer obligations regarding the processing of sensitive data, the Schrems II ruling invalidated the Privacy Shield, pointing out that these provisions were still not strong enough to prevent misuse under U.S. surveillance laws, leaving sensitive data protections particularly vulnerable.

In contrast, the DPF introduces more nuanced and stringent conditions for the processing of sensitive data, reflecting a better alignment with EU standards. It specifies broader and more specific scenarios where sensitive data processing does not require explicit consent, such as in vital interests, legal claims, medical care, employment obligations, or certain non-profit activities. Importantly, it includes provisions for journalistic exceptions and secondary liability that delineate clearer boundaries for data use in these contexts.[73] These updates represent an improvement by narrowing the conditions under which sensitive data can be processed without consent, aiming to ensure greater protection and accountability. However, critical gaps may still exist, particularly concerning the enforcement of these provisions and their interaction with U.S. law on national security and surveillance. The true test will be in the implementation and whether these updated frameworks can withstand legal scrutiny against the backdrop of international data transfers and U.S. surveillance practices.

5.2.1. Reflecting on the Core Principles of the DPF

[72] U.S. Department of Commerce, 'EU-U.S. Privacy Shield Framework' (2016) https://www.privacyshield.gov/Program-Overview accessed 18 May 2024

[73] Commission Implementing Decision (EU) 2023/4745, Annex I, Sensitive Data

The DPF represents an evolution in the approach to transatlantic data transfers, building on the foundations laid by Safe Harbor and Privacy Shield while addressing the deficiencies highlighted by the Schrems cases. Its core principles—data integrity and purpose limitation, choice, transparency, and special safeguards for sensitive data—reflect a comprehensive effort to align with the GDPR's rigorous standards.

Addressing Schrems Concerns: The explicit incorporation of GDPR standards within the DPF, particularly in relation to sensitive data, choice, and transparency, can be seen as a direct response to the vulnerabilities identified through the Schrems litigation. By emphasizing the need for affirmative consent, clear information provision, and enhanced access rights, the DPF aims to mitigate the risks associated with governmental access to data and ensure a higher level of protection for individuals' privacy.

Future Implications: The DPF builds upon the foundational elements previously established by the Safe Harbor and Privacy Shield agreements, with enhancements aimed at addressing the CJEU concerns regarding U.S. surveillance practices and the protection of EU citizens' data privacy rights. Its alignment with the GDPR principles signifies a commitment to the ongoing improvement of privacy standards. However, the framework's future implications are contingent upon its practical implementation and enforcement, as well as its ability to remain adaptable to the rapidly evolving digital landscape and the ever-changing privacy challenges it presents.

The success of the DPF in fostering a stable and secure environment for data transfers across the Atlantic will largely depend on the continued dialogue between the EU and the U.S., ensuring that the framework can dynamically adjust to new technological advancements and shifts in societal expectations around privacy. Moreover, the DPF's alignment with GDPR-like principles, while a step in the right direction, must prove its 'essential equivalence' in practice—a requirement pointed out by the CJEU to ensure that the privacy protections offered by the DPF are indeed comparable to those within the EU. This aspect highlights a significant and apparent challenge to the DPF's legal standing, pointing to the necessity for meticulous scrutiny and potential adjustments to the framework to meet this stringent standard.[74]

In essence, while the DPF aims to enhance the protection of personal data and address the critical feedback stemming from previous frameworks, its long-term effectiveness and legality remain to be seen. The cautious optimism surrounding its introduction speaks to the complexities of international data protection, highlighting the delicate balance between fostering digital trade and

[74] Andrej Savin, 'EU-US Data Privacy Framework – The New Framework for Transatlantic Data Transfers' (2023) 4 EuCML 159

ensuring durable privacy rights. As such, the future implications of the DPF will unfold within the context of its operational execution, the evolving jurisprudence of the CJEU, and the continuing efforts to bridge the gap between different legal systems and their approaches to data privacy.

5.3. Individual Rights and Enforcement Mechanisms

A) The landmark Schrems cases highlighted significant concerns regarding the adequacy of protection afforded to EU citizens' data when transferred to the U.S., particularly in relation to U.S. government access for national security purposes. In response, the DPF incorporates commitments from the U.S. to limit intelligence access to personal data and establishes new mechanisms for oversight and redress, including the DPRC and a more explicit role for DPAs. These measures aim to address the legal and societal challenges identified by the Schrems decisions, showcasing an evolved understanding of privacy rights and enforcement mechanisms in the context of transatlantic data transfers.[75]

In summary, the DPF represents an evolution in the protection of individual rights and the enforcement mechanisms available to support these rights. By building on the foundations set by Safe Harbor and Privacy Shield, particularly those critiqued in the Schrems rulings, the DPF aims to better align with the GDPR's stringent standards and strengthen the transatlantic commitment to data protection. However, the real test will be how these provisions are enacted and the extent to which they effectively mitigate past deficiencies.

5.3.1. Right of Access

The evolution of the Right of Access from Safe Harbor through Privacy Shield to the 2023 adequacy decision reflects a shift towards strengthening individuals' control over their personal data. Under Safe Harbor, the right of access was vaguely framed, often leaving individuals with limited practical ability to influence how their data was managed or to challenge inaccuracies.[76] This framework provided minimal guidance on handling access requests, which contributed to its eventual invalidation in the Schrems I ruling, where broader concerns about privacy protection inadequacies under U.S. law were central.

Privacy Shield addressed some of these deficiencies by outlining more specific rights for individuals, including the right to access personal data held by organizations, and the obligations of those organizations to provide this data clearly and expediently. However, the implementation

[75] Commission Implementing Decision (EU) 2023/4745, Redress, paras 176-178.
[76] Commission Decision 2000/520/EC [2000] OJ L215.

was still criticized for not fully respecting the fundamental nature of the access right, particularly regarding exceptions and the actual mechanisms through which access was granted. The Schrems II verdict that invalidated Privacy Shield further highlighted ongoing issues, particularly with respect to the handling of exceptions and the adequacy of protective measures against U.S. surveillance.[77]

The 2023 adequacy decision introduces a more refined and ostensibly robust framework for the Right of Access. It stresses that access should not only be granted but should be guided by the concerns leading to the request, suggesting a more nuanced and responsive approach. This includes detailed provisions for engaging with individuals to clarify and narrow their requests and ensuring that responses are tailored and timely. The decision also clearly limits the circumstances under which access can be denied, requiring organizations to justify any such restrictions transparently. This framework aims to solve past problems by reducing the arbitrary denial of access and by making the process more transparent and aligned with EU standards, such as those under the GDPR.[78] However, the practical challenges of implementing these improved standards, particularly in balancing the need to protect confidential commercial information and the right to access, remain a critical area for scrutiny. This is especially pertinent given the potential for organizations to cite burdensome processes as a loophole to deny access, despite the stipulation that costs should not be a controlling factor.

5.3.2. Redress Mechanisms

Introduction and Establishment of the DPRC

A critical advancement introduced with the DPF is the novel low threshold for admissibility of complaints and the establishment of the Data Privacy Review Court (DPRC). This approach contrasts starkly with the mechanisms provided under Safe Harbor and Privacy Shield, which were often criticized for their lack of specificity and the high barriers to accessing judicial redress for EU citizens.

Following the Schrems II ruling, the Commission initiated negotiations with the U.S. government aiming for a new adequacy decision that aligns with the standards of Article 45(2) of Regulation (EU) 2016/679 as interpreted by the Court of Justice. Consequently, the United States, on October 7, 2022, implemented Executive Order 14086 titled ‘Enhancing Safeguards for US Signals

[77] Commission Implementing Decision (EU) 2016/1250 [2016] OJ L207.
[78] Commission Implementing Decision (EU) 2023/4745, Annex I, 8, Access

Intelligence Activities'[79] (EO 14086), accompanied by a Regulation on the Data Protection Review Court enacted by the U.S. Attorney General (AG Regulation).

By highlighting limitations on intelligence gathering and introducing more rigorous oversight mechanisms, EO 14086 seeks to mitigate the tensions between privacy rights and national security interests. Furthermore, the subsequent establishment of the DPRC on 14 October 2022, through a regulation by the US Department of Justice, constitutes a pivotal element of the US's commitment to reinforcing the judicial oversight of its intelligence activities.

EO 14086 introduces a novel mechanism for addressing grievances, effectively replacing the Ombudsperson and bridging the existing gap in protection. It establishes a procedure where complaints can be filed with the Civil Liberties and Privacy Officer (CLPO), an official within the Office of the Director of National Intelligence, alongside a newly formed Data Protection Review Court. This arrangement introduces a dual-layered system for the examination of complaints aiming to provide aggrieved individuals with a means to challenge the legality of US signals intelligence activities. Initially, the CLPO has the authority to examine eligible grievances. Upon concluding its investigation, the CLPO can notify the complainant, via the relevant public authority, while maintaining confidentiality about whether the complainant was a target of U.S. signal intelligence operations, stating that: "either no violations were found, or a required corrective action has been determined by the Civil Liberties Protection Officer at the Office of the Director of National Intelligence".[80]

This first phase seems quite procedural, with little room for the application of quasi-judicial principles. Should the complainant find the resolution unsatisfactory, they have the option to seek further review by the Data Protection Review Court.

At this juncture, a special advocate is appointed to safeguard the complainant's interests throughout this stage.[81] This inclusion enhances the representation of individuals in the process, although direct involvement is still not facilitated. Individuals cannot directly interact with the new bodies established for handling complaints; instead, they must go through EU data protection authorities. The responses they get are similar to those previously given by the Ombudsperson. The Civil Liberties Protection Officer and the "Court" involved offer a standard response to complaints, without admitting or denying participation in US intelligence activities. Consequently, individuals

[79] The White House, 'Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities' (7 October 2022) https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ accessed 28 March 2024.
[80] Executive Order 14086, sec. 3(c)(E)(1) (7 October 2022)
[81] Executive Order 14086, sec. 3(c)(E)(2) (3) (7 October 2022)

remain uninformed about potential rights infringements or the specifics of any remedial actions, nor are they assured of future protections.

The results, encapsulated in a confidential report, come under the surveillance of the FISC, thus indirectly granting foreign nationals a form of access to this oversight body, despite their historical exclusion. Despite these procedural enhancements and the independent expertise of its members, skepticism remains regarding the enduring viability of this appellate mechanism as a genuine form of legal remedy, especially in light of predetermined resolutions, procedural limitations on the complainant, and the absence of further appeal options. Galehr, Stella argue that the complainants' lack of direct involvement and the non-transparent nature of the process may undermine its effectiveness.[82]

According to several authors, this system, characterized by its fixed responses and obstacles to making complaints, is not expected to meet the Court of Justice of the European Union's standards for legal remedy as outlined in Article 47 of the Charter of Fundamental Rights of the European Union.[83] Furthermore, the authors suggest that additional limits and safeguards introduced by EO 14086 may not be sufficiently clear and precise to meet the "substantially equivalent" protection requirements of Article 45 of the GDPR.[84]

Operational Independence and Compliance with EU Standards

Comprising legal experts familiar with data privacy and national security laws, and excluding current U.S. government employees from its ranks, this court allows for an impartial reevaluation of the CLPO's findings by a panel of three judges, who also consider contributions from the special advocate and adhere to pertinent U.S. Supreme Court jurisprudence.[85]

The DPRC is designed as a quasi-judicial body with the authority to review and adjudicate complaints related to the processing of personal data by US intelligence agencies, thereby offering a potential avenue for redress to aggrieved individuals.[86]

This mechanism is characterized by its accessibility, as it sets a low threshold for admissibility of complaints, not requiring individuals to demonstrate that their data was actually subject to US

[82] Galehr, Stella, Transatlantic Data Transfers under the GDPR: Developments and Outlook (Zurich Open Repository and Archive, University of Zurich 2023) https://doi.org/10.5167/uzh-252334 accessed [16.05.2024]
[83] Maximilian Schrems and noyb, 'European Commission gives EU-US data transfers third round at CJEU' (noyb.eu, 10 July 2023) https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.
[84] Sergi Batlle and Arnaud van Waeyenberge, 'EU–US Data Privacy Framework: A First Legal Assessment' (2023) European Journal of Risk Regulation
[85] Executive Order 14086, sec. 3 (d) (7 October 2022)
[86] US Department of Justice, Regulation Creating the Data Protection Review Court (14 October 2022)

surveillance[87]. This approach ostensibly broadens the scope of protection for individuals, addressing one of the critical gaps identified in the previous EU-US data transfer frameworks, such as the Privacy Shield.

A fundamental critique revolves around the DPRC's classification and operational independence.

Sergi Batlle and Arnaud van Waeyenberge stress the importance of judicial independence for the redress mechanism established under EO 14086. Citing ECtHR cases, they outline two main criteria for independence from the executive branch: judges must be appointed in their individual capacity without instructions from public authorities, and there must be safeguards against external pressure and an appearance of independence. Although the DPRC is presented as an independent tribunal, its integration within the executive branch and the method of appointment of its members—by the Attorney General of the US—raise significant questions about its neutrality and independence and this can legitimately cast doubt on its true independence from the executive.[88] Such concerns are not merely theoretical; they touch on the core principles enshrined in Article 47 of the Charter of Fundamental Rights of the European Union, which mandates access to an "effective remedy" before an independent and impartial tribunal. The critique is further compounded by the precedent set in the Schrems II judgment, where the CJEU pointed out the importance of judicial independence from the executive as a cornerstone of effective legal protection for data subjects.[89]

Moreover, the qualifications and experience required for DPRC members, while aligned with those expected in the Federal judiciary, do not in themselves guarantee the body's autonomy or mitigate the inherent conflict of interest presented by its executive branch affiliation. This regulatory boundary, which the DPRC straddles, remains a contentious issue, reflecting broader concerns about the adequacy of administrative appeals in providing protections comparable to those offered by judicial processes within the EU legal framework.[90]

This analysis leads to a critical examination of the dual-stage remedy mechanism's compliance with the CJEU's standards for independence, impartiality, and effective judicial protection. The CJEU's jurisprudence, particularly the Schrems II judgment, highlights the necessity for legal protections that are "substantially equivalent" to those afforded within the EU legal order. This

[87] Commission Implementing Decision (EU) 2023/4745, para 178
[88] Sergi Batlle and Arnaud van Waeyenberge, 'EU–US Data Privacy Framework: A First Legal Assessment' (2023) European Journal of Risk Regulation
[89] European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework (28 February 2023).
[90] Andrej Savin, 'EU-US Data Privacy Framework – The New Framework for Transatlantic Data Transfers' (2023) 4 European Data Protection Law Review 159.

benchmark is further elucidated by the European Court of Human Rights (ECtHR), which has recognized the role of specialized, non-judicial entities in delivering effective legal protection, provided they possess the requisite authority and procedural safeguards.[91]

In light of these considerations, the DPRC's establishment and the provisions of EO 14086 represent a nuanced attempt to align US surveillance practices with European privacy standards. The DPRC's operational independence, underscored by the conditions for judges' dismissal and the prohibition of concurrent government roles, reflects a concerted effort to address the CJEU's and ECtHR's criteria for judicial and quasi-judicial bodies. However, the lingering doubts about the DPRC's genuine autonomy, coupled with the procedural and substantive limitations of the redress mechanism, stressed the challenges in achieving a "substantial equivalence" in privacy protection across the Atlantic.

Gerke and Rezaeikhonakda point out three main concerns:[92]

- The DPRC is part of the executive branch, not the judiciary, which may undermine its independence.
- There is no requirement for the special advocates, who represent complainants' interests, to be independent from the executive branch.
- The DPRC's decisions are final and do not provide complainants with the right to appeal to a higher judicial authority, which could violate the right to effective judicial protection under EU law.

The establishment of the DPRC and the procedural mechanisms it introduces, including the finality of its decisions and the requirement for thorough rationales, signify a concerted effort to enhance accountability and redress in the context of US intelligence surveillance. These measures, detailed in Executive Order 14086, represent an attempt to address some of the criticisms leveled against the US's approach to data protection in the aftermath of the Schrems II verdict. However, the exclusive control over the appointment process vested in the executive branch, as well as the lack of a clear judicial appeal path, pose significant challenges to the perceived independence and impartiality of the DPRC. These aspects may not fully align with the European standards for judicial protection and could potentially undermine the framework's legitimacy in the eyes of European authorities and data subjects.[93]

[91] ECtHR, Klass and others v Germany, App no 5029/71 (6 September 1978).
[92] Sara Gerke and Delaram Rezaeikhonakdar, 'Privacy Shield 2.0 — A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States' (2023) 45(2) Cardozo Law Review (published February 2024).
[93] A Savin, 'The New Framework for Transatlantic Data Transfers' CBS LAW Research Paper No. 23-01, 12.

Moreover, the broader implications of these developments cannot be overlooked. The dialogue between the US and the EU on data protection and privacy standards is situated within a larger context of global digital governance, where differing legal systems and cultural values often collide. The attempts to bridge these differences through frameworks like the DPF and mechanisms like the DPRC are indicative of a shared commitment to facilitating transatlantic data flows while respecting the fundamental rights of individuals. Yet, the challenges highlighted in the assessments of the EDPB and the European Parliament illustrate the inherent difficulties in translating this commitment into practical, universally acceptable solutions.

In conclusion, the establishment of the DPRC under Executive Order 14086 represents a step forward in the effort to reconcile US intelligence practices with European privacy standards. However, the concerns raised by European institutions regarding the DPRC's independence, the adequacy of the redress mechanisms, and the overall compatibility of the EU-US Data Privacy Framework with EU data protection laws underline the ongoing challenges in achieving a balanced and effective approach to transatlantic data protection. It remains imperative for the Commission to closely monitor the implementation of these mechanisms and to be prepared to adjust the framework as necessary to ensure that it offers protections that are not just nominal but are substantively equivalent to those afforded within the EU. This ongoing evaluation and adaptation process is crucial in upholding the rights of individuals and maintaining trust in the mechanisms governing transatlantic data flows.

5.3.3. Cooperation with Data Protection Authorities (DPAs)

Under the previous frameworks such as Safe Harbor and Privacy Shield, cooperation with EU DPAs was encouraged but often criticized for lacking substance and secure mechanisms for real-time and effective collaboration. These frameworks offered general promises of cooperation without specifying the depth of coordination, often resulting in criticism for ineffective handling of complaints and enforcement actions. The European Court of Justice's decisions in Schrems I and II underscored the deficiencies in transatlantic data protection enforcement, particularly highlighting the need for more substantive and operative collaboration mechanisms.

The new 2023 adequacy decision takes steps to address these past criticisms by embedding structured and specific cooperation protocols within the EU-U.S. Data Privacy Framework. The FTC's commitment to exchanging information on referrals, providing status updates, and engaging

in evaluative discussions about significant issues marks a proactive approach to enforcement cooperation. The inclusion of the SAFE WEB Act's provisions, allowing the FTC to issue compulsory process on behalf of EU DPAs and to share investigatory information, represents a practical tool that directly supports EU DPAs in their enforcement efforts. This kind of legislative backing significantly enhances the operational capacity for handling data protection cases collaboratively across borders.[94]

However, while these mechanisms are a clear improvement in theory, their efficacy in practice remains to be tested. The effectiveness of such cooperation is contingent on the ongoing commitment of U.S. authorities to prioritize privacy issues at the level demanded by EU standards, which is challenging given the broader U.S. legal landscape that includes significant national security interests that have previously overridden privacy concerns. Moreover, the FTC's ability to provide meaningful, timely assistance is constrained by legal and practical considerations such as confidentiality laws and the actual capacity to handle numerous international referrals efficiently. Galehr, Stella point out that the FTC does not have authority over all companies, particularly exempting sectors like financial institutions, air carriers, and telecommunications companies. This limitation could impact the overall enforcement effectiveness of the DPF and its ability to provide comprehensive data protection.[95] These challenges highlight that while the new framework addresses some of the structural weaknesses of past agreements, achieving the desired level of transatlantic data protection cooperation depends heavily on sustained commitment and resource allocation by the FTC, alongside reciprocal and reliable engagement from EU DPAs.

5.4. Surveillance and Government Access to Data: An Analysis within the Data Privacy Framework (DPF) Context

5.4.1. Introduction to Surveillance and Government Data Access

The Digital Age has necessitated durable frameworks for the transatlantic transfer of personal data, with evolving challenges in balancing national security interests and individual privacy rights. The DPF emerges as a pivotal advancement in this arena, addressing concerns previously highlighted

[94] Commission Implementing Decision (EU) 2023/4745, Annex IV, IV 'Enforcement Cooperation with EU DPAs'
[95] Galehr, Stella, Transatlantic Data Transfers under the GDPR: Developments and Outlook (Zurich Open Repository and Archive, University of Zurich 2023) https://doi.org/10.5167/uzh-252334 accessed [16.05.2024]

by the Safe Harbor and Privacy Shield frameworks. This section delves into the U.S. commitments under the DPF to limit intelligence access to personal data, contrasts these with the safeguards under Safe Harbor and Privacy Shield, and considers the implications of the Schrems cases on these developments.

Evolution from Safe Harbor to Privacy Shield

Initially, the Safe Harbor agreement was criticized for its inadequate protection against U.S. surveillance practices. The European Court of Justice (ECJ) invalidated it in the Schrems I case, citing concerns over mass surveillance by U.S. intelligence agencies without adequate redress mechanisms for EU citizens. The Privacy Shield sought to address these shortcomings by introducing more stringent data protection commitments and oversight mechanisms. However, it too was eventually deemed insufficient in the Schrems II ruling, primarily due to the ongoing potential for indiscriminate surveillance by U.S. authorities.

DPF's Legal Commitments and Proportionality

The DPF incorporates explicit U.S. legal commitments to limit arbitrary or unjustified access to data. Annex VI of the DPF emphasizes the importance of judicial oversight and the adherence to the Fourth Amendment, ensuring a legal basis and proportionality in government access to personal data.[96] These commitments indicate a strategic alignment with the GDPR's principles, aiming to mitigate the concerns that led to the invalidation of its predecessors.

Oversight Mechanisms for Law Enforcement and Surveillance Activities

The DPF introduces comprehensive oversight mechanisms, including judicial and non-judicial bodies to supervise law enforcement and surveillance activities. This multifaceted oversight aims to ensure compliance with stringent data protection standards, providing a structured framework that surpasses the mechanisms under Safe Harbor and Privacy Shield.[97]

5.4.2. Analysis of U.S. Commitments under the DPF

Despite its ambition, EO 14086, functioning as an executive action, raises concerns regarding its ability to mandate comprehensive compliance across various federal departments, including intelligence agencies. Its alignment with EU principles is complicated by the existing legal framework in the U.S., notably the Foreign Intelligence Surveillance Act (FISA) and its Article 702. This legislation permits the monitoring of non-U.S. citizens overseas, presenting a legal conundrum in adhering to the principles of "necessity" and "proportionality" as interpreted in the

[96] Commission Implementing Decision (EU) 2023/4745, Annex I
[97] Commission Implementing Decision (EU) 2023/4745, sec 3.1.2 'Oversight'

Charter's Articles 7 and 52, and Article 8 of the European Convention on Human Rights. The Charter stipulates that restrictions on fundamental rights require a clear legal basis, a standard FISA's current form struggles to meet without legislative amendment, a perspective echoed by the European Parliament.[98]

EO 14086 introduces amendments to the Department of Justice regulations and establishes the DPRC, aiming to provide enhanced safeguards against national security access to personal data. These measures signify a comprehensive approach, addressing the criticisms from the Court of Justice of the European Union and focusing on integrating privacy and civil liberties into intelligence activities planning.[99]

However, the authorization for surveillance, as delineated in EO 14086, extends beyond legal statutes to include executive orders and presidential directives, potentially bypassing the stringent necessity for surveillance activities to be the only method to achieve a particular aim. This expansion allows for surveillance to be considered the most effective solution by presidential decree, raising questions about the adherence to EU standards of necessity and proportionality.[100]

Sara Gerke and Delaram Rezaeikhonakda argue that while these changes are an improvement, they do not fully align with the stricter interpretations of necessity and proportionality under EU law. The U.S. interpretation of these principles remains broader and may not satisfy the requirements of the CJEU, which could jeopardize the adequacy decision under the GDPR.[101]

Critics, such as the group noyb led by Maximilian Schrems, quickly pointed out that while Executive Order 14086 requires large-scale data collection to be "proportionate," there is a lack of shared understanding between the EU and the US on what this actually means in practice. Initially, the Court of Justice of the European Union (CJEU) found that the US's broad surveillance under FISA 702 did not meet the European Union's standards for being "proportionate" as defined by the EU's Charter of Fundamental Rights, Article 52. However, the recent US Executive Order 14086, which follows the principles of PPD-28 from 2014, includes the term "proportionate." But, the US gives a different meaning to "proportionate" than the CJEU does. Executive Order 14086 claims that the US's broad surveillance is "proportionate" under a definition that is unique to the US,

[98] Charter of Fundamental Rights of the European Union [2000] OJ C364/01, art 52.
[99] Commission Implementing Decision (EU) 2023/4745, paras 142-152, 'Legal bases, limitations and safeguards'
[100] Executive Order (n 22), Secs 2(a)(i), 2(a)(ii)(A))
[101] Sara Gerke and Delaram Rezaeikhonakdar, 'Privacy Shield 2.0 — A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States' (2023) 45(2) Cardozo Law Review (published February 2024).

differing from the EU's interpretation. This allows both the EU and US to say they agree on the term "proportionate," even though they understand it differently.[102]

The Executive Order specifies processing objectives in both affirmative and negative terms, setting forth legitimate goals across a broad spectrum, including foreign intelligence gathering and addressing global challenges. However, it explicitly excludes objectives that could undermine freedom of expression or provide competitive advantages through espionage. Despite these provisions, the authorization for bulk collection under certain circumstances without prior authorization diverges from the standards set by the European Commission, emphasizing the challenges in aligning U.S. intelligence practices with EU norms.[103]

The Schrems II ruling underlined that Article 702 of FISA fails to meet the EU's proportionality criterion by not limiting its granted powers and lacking "clear and precise rules" for its implementation. This highlights the fundamental challenge of ensuring that U.S. surveillance practices conform to the stringent standards set by the EU, particularly in the context of protecting fundamental rights and providing a legal foundation for restrictions, as required by the Charter of Fundamental Rights.[104]

In April 2024, the U.S. Congress passed significant reforms to Section 702 of FISA through the Reforming Intelligence and Securing America Act. This critical legislation, heralded by President Biden as a tool to "understand and protect against a wide range of dangerous threats," was signed into law under immense pressure, just before its expiration.[105] Despite its primary aim to facilitate intelligence on non-Americans outside the U.S., the Act has stoked considerable debate from an EU perspective, particularly regarding the General Data Protection Regulation. The reforms introduce enhanced safeguards for privacy and civil liberties, including codifying measures the Justice Department previously adopted. Yet, concerns linger about the incidental collection of EU citizens' data and the potential for their rights under the GDPR to be undermined without adequate safeguards. These developments pose a complex challenge for transatlantic data privacy agreements, as the EU continues to demand stringent protections aligned with its fundamental values and legal standards.

---

[102] Maximilian Schrems and noyb, 'European Commission gives EU-US data transfers third round at CJEU' (noyb.eu, 10 July 2023) https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu
[103] Draft Commission Implementing Decision on the EU-US Data Privacy Framework, Preamble, para 134
[104] Schrems II (n 6) paras 180, 181
[105] White House, 'Statement from National Security Advisor Jake Sullivan on the Senate's Vote on the Reauthorization and Reform of FISA Section 702' (White House, 20 April 2024) https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/20/statement-from-national-security-advisor-jake-sullivan-on-the-senates-vote-on-the-reauthorization-and-reform-of-fisa-section-702/

In summary, while Executive Order 140 86 and the establishment of the Data Protection Review Court (DPRC) represent significant strides toward enhancing privacy protections and addressing the EU's concerns post-Schrems II, the path to full compliance and reconciliation with EU standards reveals intricate challenges. Central to these challenges is the inherent tension between the broad executive powers under U.S. law and the EU's rigorous demands for a legal framework that strictly adheres to principles of necessity and proportionality in intelligence gathering.

The role of oversight mechanisms, including the PCLOB and the DPRC, is critical in this context. These bodies are tasked with ensuring that executive actions and intelligence activities are conducted with a high regard for privacy and civil liberties, a mandate that aligns with the objectives of EO 14086. Nevertheless, the effectiveness of these oversight mechanisms, along with the operational transparency of the Foreign Intelligence Surveillance Court (FISC) and its appellate body, the FISCR, remains a subject of debate. The historical rarity of warrant application rejections and the procedural opacity of these courts raise valid concerns about the robustness of the safeguards in place.[106]

Moreover, the Executive Order's ambitions are somewhat curtailed by the existing legislative framework, notably FISA and its contentious Article 702. The Schrems II judgment critically points out that the current U.S. legal structure, without significant legislative amendments, falls short of the EU's Charter of Fundamental Rights, particularly concerning the limitation of powers and the establishment of clear and precise rules for surveillance activities. The European Parliament remains skeptical, advocating for legislative changes to ensure the fundamental rights of individuals are not overshadowed by national security interests.[107]

The Executive Order's directive for processing objectives and the establishment of limitations, including the provision for bulk collection under specific conditions, reflects an attempt to balance national security interests with privacy concerns. However, the divergence from EU standards, especially regarding data minimization and the explicit exclusion of objectives that undermine freedom of expression, indicates a complex negotiation between operational necessity and the protection of civil liberties.[108] Sara Gerke and Delaram Rezaeikhonakdar highlight that EO 14086 imposes limitations on the bulk collection of signals intelligence by requiring a determination that the necessary information cannot reasonably be obtained through targeted collection. This represents a step forward compared to PPD-28, which did not prioritize targeted collection over

[106] Privacy International (n 39) para 44
[107] European Parliament resolution of 20 May 2021 and the draft motion for a resolution of the Committee on Civil Liberties, Justice and Home Affairs on 14 February 2023
[108] European Commission, Draft Commission Implementing Decision on the adequate protection level of personal data under the EU-US Data Privacy Framework (13 December 2022), Preamble para 134

bulk collection. Despite these advancements, Gerke and Rezaeikhonakda express concerns that the U.S. criteria for bulk collection—based on advancing a validated intelligence priority—remain too broad and may not comply with EU standards. The permissibility of bulk collection under EO 14086 is seen as potentially conflicting with the stricter EU interpretations of data protection rights.[109]

In conclusion, while Executive Order 14086 embodies a proactive approach to aligning U.S. intelligence practices with EU data protection standards, its implementation and the broader legal and regulatory framework present substantial hurdles. The juxtaposition of U.S. national security interests with the EU's stringent privacy requirements necessitates a nuanced approach that respects the legal and operational complexities inherent in transatlantic data flows. The evolution of this framework and its reconciliation with EU standards will undoubtedly require ongoing dialogue, legislative consideration, and a commitment to ensuring the protection of fundamental rights in the digital age.

5.4.3. Comparative Analysis with Safe Harbor and Privacy Shield

The DPF's approach to surveillance and government data access presents an advancement over its predecessors. While Safe Harbor and Privacy Shield offered initial frameworks for addressing these issues, their mechanisms were ultimately found lacking in the face of ECJ scrutiny. The DPF, with its detailed legal bases, oversight structures, and redress mechanisms, represents a more resilient and legally sound framework designed to withstand similar judicial evaluations.

Addressing Schrems Concerns

The Schrems cases highlighted the critical need for substantial protections against mass surveillance and for effective judicial redress mechanisms for EU citizens. The DPF directly addresses these concerns by establishing clear legal limitations on surveillance activities, incorporating principles of necessity and proportionality, and providing EU individuals with avenues for redress. This targeted response signifies an essential shift towards reconciling U.S. intelligence gathering with EU data protection standards.

The DPF signifies a significant evolution in the U.S.-EU data transfer framework, specifically addressing the challenges related to surveillance and government access to data. By integrating

[109] Sara Gerke and Delaram Rezaeikhonakdar, 'Privacy Shield 2.0 — A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States' (2023) 45(2) Cardozo Law Review (published February 2024).

rigorous legal commitments, oversight mechanisms, and redress avenues, the DPF aims to provide a resilient and legally solid framework that addresses past criticisms and aligns with the GDPR's stringent data protection standards. As such, it marks a critical step forward in the ongoing effort to balance national security interests with the fundamental right to privacy.

The DPF's design explicitly aims to address the core issues raised by the Schrems cases, particularly regarding surveillance practices and the lack of effective judicial redress for EU citizens. By incorporating stringent safeguards and establishing clear, enforceable rights for individuals, the DPF demonstrates a commitment to reconciling the needs of national security with the rights of individuals to data protection and privacy. This balance is crucial for the framework's long-term viability and acceptance, both legally and socially, within the EU.

The DPF's foundational strength lies in its comprehensive legal framework, which directly addresses the deficiencies identified in both the Safe Harbor and Privacy Shield agreements. By establishing more explicit and enforceable safeguards against indiscriminate surveillance, the DPF offers a level of protection that more closely aligns with the European Union's stringent data protection standards. Notably, the introduction of Executive Order 14086 and the establishment of the Data Protection Review Court (DPRC) are pivotal advancements. These mechanisms not only set limitations on signals intelligence activities but also provide an unprecedented level of judicial oversight and the possibility of redress for individuals affected by data collection practices. This dual approach of limitation and oversight represents a significant advantage over previous frameworks, offering clearer, stronger protections for personal data transferred across the Atlantic.

Challenges and Opportunities

While the DPF represents a significant step forward, it is not without its challenges. The framework's effectiveness in practice will depend on its implementation and the ongoing commitment of U.S. authorities to uphold these standards. Additionally, future legal challenges could test the DPF's resilience, particularly in how effectively the DPRC functions as a mechanism for redress. Moreover, the dynamic nature of technology and international relations may necessitate continual adjustments to the framework to maintain its adequacy in protecting personal data.

The DPF also presents opportunities, particularly in restoring trust in transatlantic data flows, essential for economic and security cooperation between the EU and the U.S. By providing a stable legal basis for data transfers, the DPF can facilitate business operations and innovation while ensuring that individuals' data protection rights are respected. Furthermore, the DPF could serve

as a model for other international data transfer agreements, potentially influencing global data protection standards and practices.

The adoption of the DPF marks a crucial juncture in the ongoing dialogue between the EU and the U.S. on data protection and privacy. As the framework is implemented and tested, its real-world impact on surveillance practices and individual rights will become clearer. Continuous monitoring, evaluation, and adaptation will be essential to ensure that the DPF remains effective in the face of evolving challenges and technological advancements.

The DPF's success will also depend on the sustained engagement and cooperation between EU and U.S. authorities, ensuring that the framework's provisions are not only formally adopted but also actively enforced. This collaborative effort will be vital in maintaining the integrity of the DPF and ensuring that it continues to serve as a foundation for transatlantic data transfers.

The DPF represents an evolution in the framework for transatlantic data transfers, aiming to address the complex challenges of surveillance and government access to data. By establishing clearer legal safeguards, oversight mechanisms, and avenues for redress, the DPF seeks to provide a more secure and privacy-respecting environment for the transfer of personal data. While challenges remain, the DPF's comprehensive approach offers a promising path forward in harmonizing data protection standards between the EU and the U.S., ultimately enhancing the protection of individual rights in the digital age.

6. Impact on Businesses and Compliance Requirements

In the evolution of data transfer frameworks between the EU and the US, businesses have faced evolving compliance obligations aimed at safeguarding personal data. The transition from the Safe Harbor Agreement to the Privacy Shield, and finally to the DPF, reflects a continuous effort to strengthen data protection standards in response to legal, societal, and technological changes. This section delves into the detailed comparison of compliance obligations across these three frameworks, highlighting the DPF's requirements for continuous protection and the annual recertification process, against the backdrop of the problems raised by the Schrems cases.

Compliance Evolution: From Safe Harbor to DPF

Safe Harbor: Instituted in 2000, the Safe Harbor framework was the first mechanism that allowed US businesses to comply with EU data protection requirements for transatlantic data transfers. Compliance was largely based on a self-certification process where US companies pledged adherence to seven principles resembling those of the EU Data Protection Directive (Directive 95/46/EC). However, the framework provided limited enforcement mechanisms, and its self-regulatory nature was criticized for offering inadequate protection.

Privacy Shield*:* In response to the European Court of Justice's invalidation of the Safe Harbor framework in the Schrems I case (2015), the EU-US Privacy Shield was established in 2016. The Privacy Shield introduced stronger mechanisms for oversight, including greater enforcement roles for the US Department of Commerce and the Federal Trade Commission, as well as the establishment of a new Ombudsperson mechanism for handling EU citizens' complaints regarding data access by US intelligence agencies. It also mandated more detailed privacy policies and clearer recourse mechanisms for individuals, setting a higher standard for data protection.

Data Privacy Framework: The DPF, succeeding the Privacy Shield, seeks to address the criticisms and legal shortcomings exposed by the Schrems II decision (2020), which invalidated the Privacy Shield. The DPF incorporates stringent compliance obligations, stressing continuous protection of data, operationalizing GDPR-like standards within the US framework, and introducing an annual recertification process to ensure ongoing adherence to privacy principles.

Detailed Compliance Obligations under the DPF

The DPF outlines comprehensive compliance obligations for US businesses handling EU data, significantly expanding on the requirements of its predecessors:

- **Legal Process and Financial Implications:** The DPF provides detailed descriptions of various legal processes (such as grand jury subpoenas and search warrants) and their

implications for US businesses. Notably, violations of the FTC's administrative orders can result in civil penalties up to $50,120 per violation, per day, underscoring the strict compliance landscape under the DPF.[110]

- **Continuous Protection and Annual Recertification**: A pivotal requirement under the DPF is the obligation for continuous protection of EU data and an annual recertification of compliance. This necessitates that businesses not only adhere to the DPF principles at the point of certification but also maintain these standards consistently, demonstrating a commitment to data protection that extends beyond the initial certification process.[111]
- **Monitoring and Verification:** The DPF mandates ongoing compliance monitoring through mechanisms like 'spot checks' and ad hoc reviews by the DoC. This proactive approach ensures that businesses continuously meet the DPF standards, with actions upon non-compliance leading to potential enforcement actions by the FTC or Department of Transportation.[112]
- **Accountability and Record-Keeping:** Reflecting the GDPR's focus on accountability, the DPF requires businesses to implement appropriate technical and organizational measures for data protection and to demonstrate compliance through record-keeping. These records must be available upon request in investigations or complaints, reinforcing the framework's accountability principle.[113]
- **Restrictions on Onward Transfers:** The DPF imposes restrictions on the onward transfer of personal data, ensuring that the level of protection is not compromised. Specific conditions apply, especially when transferring data to third parties or for different purposes, necessitating detailed contractual provisions to safeguard privacy.[114]

Schrems Cases: Implications for Compliance

The Schrems cases (I and II) have had a profound impact on the evolution of transatlantic data transfer frameworks, highlighting the need for stable privacy protections and effective enforcement mechanisms. Schrems I led to the demise of Safe Harbor, while Schrems II invalidated the Privacy Shield, criticizing its inability to protect EU citizens' data from US surveillance practices. The DPF aims to address these concerns by implementing stronger

[110] Commission Implementing Decision (EU) 2023/4745, Annex IV, III.
[111] Commission Implementing Decision (EU) 2023/4745, 2.1.2 (9).
[112] Commission Implementing Decision (EU) 2023/4745, 2.3.2 (53)
[113] Commission Implementing Decision (EU) 2023/4745, 2.2.7 (44-46)
[114] Commission Implementing Decision (EU) 2023/4745, 2.2.6 (37-43).

safeguards against surveillance, ensuring data protection aligns with EU standards, and introducing more rigorous compliance and enforcement mechanisms.

Enhanced Compliance and Enforcement under the DPF

Enhanced Safeguards Against Surveillance: A critical focus of the DPF is to limit U.S. intelligence agencies' access to personal data, responding directly to the concerns raised in the Schrems II decision. The tries to establish clear limitations and safeguards on data access for national security purposes, requiring transparency and oversight of surveillance activities. This represents a shift from the earlier frameworks, aiming to align U.S. practices more closely with EU standards on government access to data.[115]

Operationalization and Supervision: The DPF points out the operationalization of privacy protections, detailing the Department of Commerce's commitment to administering and supervising the program. This includes verification of self-certification requirements and cooperation with European Data Protection Authorities (DPAs). Such measures demonstrate a proactive approach to ensuring compliance, significantly beyond the self-regulatory model of Safe Harbor and enhancing the more structured framework of the Privacy Shield.[116]

Proactive Enforcement Efforts: The DPF signals a shift towards more proactive enforcement efforts, as evidenced by the focus on types of substantive violations highlighted in cases like Twitter[117], Flo[118]. This indicates an intention to actively pursue violations of the DPF principles, reinforcing the commitment to a high standard of data protection. Moreover, the stipulation that organizations may be subject to enforcement even if they fail to maintain their self-certification highlights the continuous nature of compliance obligations under the DPF.[119]

Implications for Businesses: The DPF imposes a comprehensive set of obligations on U.S. businesses, demanding a continuous commitment to data protection and a structured process for annual recertification. This includes a detailed understanding of legal processes affecting data transfers, stringent monitoring and verification of compliance, and adherence to enhanced safeguards against surveillance. Businesses must also navigate the restrictions on onward transfers with greater caution, ensuring that any further data movement complies with the DPF's stringent requirements.

---

[115] Commission Implementing Decision (EU) 2023/4745, Art 3(3)
[116] Commission Implementing Decision (EU) 2023/4745, ANNEX III
[117] In the Matter of Twitter, Inc., a Corporation, FTC File No. 092 3093, Agreement Containing Consent Order (11 March 2011)
[118] In the Matter of Flo Health, Inc., FTC File No. 192 3133, Agreement Containing Consent Order (13 January 2021).
[119] Commission Implementing Decision (EU) 2023/4745, ANNEX IV

Comparative Analysis: When compared to Safe Harbor and Privacy Shield, the DPF represents an evolution in terms of compliance obligations, enforcement mechanisms, and protections against U.S. surveillance. The framework's focus on continuous protection, operational oversight, and proactive enforcement reflects a response to the criticisms highlighted by the Schrems decisions, aiming to establish a more resilient framework for transatlantic data transfers.

Conclusion

The adoption of the DPF marks an important step in the ongoing effort to align U.S. data protection standards with those of the EU, addressing past criticisms while setting a forward-looking agenda for privacy and data protection. For businesses, the transition to the DPF requires a thorough reassessment of compliance strategies, with a focus on continuous protection, operational adherence to privacy principles, and engagement in the annual recertification process. As the landscape of international data transfers continues to evolve, the DPF provides a framework that addresses the immediate concerns raised by the Schrems cases and enhances transatlantic privacy cooperation.

6.1. Exceptions to Adherence and Shared Enforcement Responsibility

The DPF represents the latest effort to regulate data transfers between the European Union and the United States, building on the foundations laid by its predecessors, Safe Harbor and Privacy Shield. These frameworks have been pivotal in facilitating transatlantic data flows, striving to uphold European citizens' data protection rights within the U.S. Each framework has evolved to address the shifting landscape of privacy concerns and legal standards, with the DPF embodying the culmination of these efforts to offer reliable data protection and privacy standards.

Under the DPF, exceptions to strict adherence are carefully circumscribed, reflecting updates for contemporary privacy concerns and legal requirements. The DPF allows for limited deviations from its principles under specific conditions, such as legal obligations or matters of national security, similar to the provisions found in Safe Harbor and Privacy Shield. This continuity underscores an ongoing effort to balance privacy rights against other societal needs.[120]

Moreover, the DPF emphasizes the necessity of demonstrating that any non-compliance with its principles is strictly required to meet overriding legitimate interests. It encourages organizations

[120] Commission Implementing Decision (EU) 2023/4745, Annex I, i, ii.

to seek the highest possible protection level where U.S. law allows, aiming for transparency and full implementation of its principles. This approach marks a deliberate effort to more explicitly balance privacy protections with other legal obligations.[121]

Specific scenarios under the DPF's supplemental principles address instances where adherence to the primary principles may not be feasible, such as in the processing of sensitive data or under journalistic exceptions. These acknowledgments recognize the complex interplay between data processing requirements and other fundamental rights, offering a pragmatic approach to data protection.[122]

The framework also delineates conditions under which performing due diligence and conducting audits without consent may be necessary, echoing similar provisions in the Privacy Shield but with enhanced specificity. This reflects an understanding of the practical necessities for certain data processing activities within the bounds of legal compliance or legitimate business interests.[123]

An evolution within the DPF pertains to the role of Data Protection Authorities and the enforcement mechanisms it establishes. Compared to Safe Harbor and Privacy Shield, the DPF augments the cooperative framework for resolving complaints and ensuring compliance, indicating a broader trend towards more stringent enforcement of data protection principles.[124]

In conclusion, the transition from Safe Harbor through Privacy Shield to the DPF illustrates an enhancement of data protection frameworks, with the DPF aiming to provide a comprehensive and nuanced mechanism for EU-U.S. data transfers. By elaborating on exceptions and highlighting a balanced approach to privacy protections, the DPF seeks to address the complexities of modern data processing within a framework of solid privacy standards.

6.2. Enhanced Collaborative Enforcement in the Data Privacy Framework: Bridging the Divide between Privacy Protections and Governmental Surveillance Post-Schrems

The shared enforcement responsibility under the DPF, against the backdrop of the Schrems decisions, highlights a concerted effort to enhance protections against government surveillance

[121] Commission Implementing Decision (EU) 2023/4745, Annex I, para 5
[122] Commission Implementing Decision (EU) 2023/4745, Annex I, III.2 'Supplemental Principles'
[123] Commission Implementing Decision (EU) 2023/4745, Annex I, III 'Supplemental Principles on Performing Due Diligence and Conducting Audits'.
[124] Commission Implementing Decision (EU) 2023/4745, Annex IV, IV 'Enforcement Cooperation with EU DPAs'.

and to strengthen enforcement mechanisms. By delineating clear roles for both governmental bodies and the private sector, the DPF aims to establish a solid foundation for personal data protection, addressing the inadequacies noted in its predecessors.[125]

Governmental roles in enforcement are significantly bolstered within the DPF, with clear commitments to limit data access for national security purposes and to engage in active cooperation between the FTC and European DPAs. This represents a direct response to concerns raised by the European Court of Justice in the Schrems II decision, emphasizing a more rigorous and collaborative approach to enforcement.[126]

On the private sector side, the DPF points out the importance of self-regulation and adherence to privacy principles through self-certification processes. It introduces stringent mechanisms for monitoring compliance and addressing false claims, thereby reinforcing the accountability of private entities in upholding data protection standards.[127]

By addressing the need to balance privacy protections with other societal needs, the DPF delineates clear exceptions and conditions for data transfers, seeking to reconcile data protection with national security and law enforcement requirements. This nuanced approach aims to ensure that the DPF can provide a legally robust and flexible framework capable of accommodating the complex interplay between privacy rights and other public interests.

The evolution of the DPF from its predecessors marks a step forward in transatlantic data protection, reflecting a deepened commitment to addressing the criticisms and challenges highlighted by the Schrems cases. Through enhanced roles for governmental bodies and the private sector, alongside clearer mechanisms for cooperation and redress, the DPF aims to establish a more effective and resilient framework for the protection of personal data transferred across the Atlantic. This model of shared enforcement responsibility, refined through the experiences of Safe Harbor and Privacy Shield and in response to legal challenges such as the Schrems cases, demonstrates a comprehensive effort to balance privacy protections with other societal needs. It signifies an advancement toward ensuring that transatlantic data transfers are conducted within a framework that respects the privacy rights of individuals while also considering the legitimate needs of national security and law enforcement.[128]

Concluding Remarks

[125] Commission Implementing Decision (EU) 2023/4745, Annex I, para 15c.
[126] Commission Implementing Decision (EU) 2023/4745, 'Effects of This Decision and Action of Data Protection Authorities' (207).
[127] Commission Implementing Decision (EU) 2023/4745, 2.3.3 (57).
[128] Commission Implementing Decision (EU) 2023/4745, Annex I, III.3 'Supplemental Principles. Annex IV

The DPF's detailed approach to exceptions and enforcement, with explicit provisions for demonstrating the necessity of non-compliance in certain scenarios and for engaging in a cooperative enforcement model, highlights the nuanced understanding that has developed around data protection. This understanding acknowledges that effective privacy framework enforcement requires collaboration between the private sector and governmental entities, leveraging their respective strengths to achieve comprehensive privacy protection.[129]

Moreover, the DPF's focus on balancing privacy protections with other societal needs through delineated exceptions underscores a commitment to a more nuanced legal framework. It acknowledges the complexities of data processing in the modern world, offering practical solutions that respect fundamental rights while accommodating the realities of national security, law enforcement, and legitimate business practices.[130]

In conclusion, the Data Privacy Framework represents a step forward in the evolution of EU-U.S. data transfer mechanisms, building upon the lessons learned from Safe Harbor and Privacy Shield to address contemporary challenges. By establishing a shared enforcement model that stresses the roles of both the private sector and governmental bodies, the DPF aims to provide a stable, legally strong foundation for transatlantic data protection. This approach reflects an acknowledgment of the criticisms and challenges highlighted by the Schrems cases, moving towards a framework that balances the need for data protection with other important societal considerations. Through its detailed exceptions, enforcement mechanisms, and emphasis on cooperation, the DPF seeks to ensure the ongoing protection of privacy rights in the face of evolving legal, technological, and societal landscapes.

The Data Privacy Framework's adoption demonstrates a commitment to refining and strengthening transatlantic data protection measures in response to evolving challenges and legal precedents. By integrating feedback from previous frameworks and legal rulings, particularly the Schrems decisions, the DPF aims to reconcile the demands of privacy protection with the realities of global data flows, national security concerns, and the digital economy.

The DPF's nuanced approach to exceptions and adherence, specifying conditions under which deviations from its principles are permissible, illustrates a sophisticated understanding of the interplay between privacy rights and other societal needs. This includes acknowledging the importance of national security and public interest while ensuring that such considerations do not unduly compromise individual privacy rights. The framework's detailed guidelines for claiming

[129] Commission Implementing Decision (EU) 2023/4745, 2.3.3 (57); Annex I, g.
[130] Commission Implementing Decision (EU) 2023/4745, Annex I, i, ii

exceptions, along with its stress on transparency and accountability, represent a concerted effort to maintain trust in the mechanisms governing transatlantic data transfers.[131]

Furthermore, the DPF strengthens the enforcement paradigm through a shared responsibility model, clearly delineating the roles of both the private sector and governmental bodies. This model includes provisions for cooperation between U.S. agencies, such as the FTC, and European Data Protection Authorities (DPAs), enhancing the ability to address violations and ensure compliance effectively. Such cooperation is pivotal for the DPF's success, as it bridges the regulatory and enforcement gaps that previously undermined the Safe Harbor and Privacy Shield frameworks. By fostering a collaborative environment for enforcement and redress, the DPF seeks to offer a more resilient and responsive framework capable of adapting to the complex landscape of global data protection.[132]

The DPF's introduction of more rigorous monitoring and verification mechanisms to address false claims of compliance also reflects a significant advancement in enforcement efforts. These mechanisms aim to prevent misuse of the framework and ensure that organizations that fail to adhere to its principles are held accountable. This focus on accountability and verifiable compliance is a direct response to the challenges identified in the Schrems rulings, emphasizing the importance of enforcement in maintaining the integrity of transatlantic data protection efforts.[133]

By articulating a clear strategy for balancing privacy protections with other societal needs, the DPF acknowledges the multifaceted nature of data protection in a global context. It recognizes that effective privacy frameworks must accommodate a range of interests, from individual privacy rights to national security and economic considerations.

In summary, the DPF embodies a sophisticated and adaptable framework for EU-U.S. data transfers, addressing the critiques and legal challenges that led to the demise of its predecessors. By emphasizing shared enforcement responsibility, detailed exceptions, and enhanced cooperation between regulatory bodies, the DPF aims to establish a durable foundation for protecting privacy rights while accommodating the complex realities of international data flows. This approach reflects a deepened understanding of the critical balance required between safeguarding privacy and enabling the transatlantic digital economy, marking a significant step forward in the evolution of data protection standards and practices.

---

[131] Commission Implementing Decision (EU) 2023/4745, Annex I, i, ii
[132] Commission Implementing Decision (EU) 2023/4745, Annex I, III.3 'Supplemental Principles'; and Annex IV
[133] Commission Implementing Decision (EU) 2023/4745, 2.3.3 (57).

6.3. Certifying Compliance under the DPF

The certification process under the DPF, signifies a critical milestone in this journey, incorporating rigorous self-certification requirements and verification mechanisms to ensure organizations' compliance with the framework's stringent data protection standards. This section of the thesis delves into the certification process mandated by the DPF, highlighting its significance in the context of transatlantic data transfers and its evolution from previous frameworks.

Under the new adequacy decision, organizations are required to adhere to a comprehensive set of requirements to self-certify. This marks an evolution in data protection standards and practices, reflecting a shift from the principles-based approach of Safe Harbour to more structured commitments under Privacy Shield, and now to the detailed and rigorous self-certification process under the DPF. Initially, organizations had to adhere to a broad framework, focusing on adherence to principles without stringent verification or annual recertification mandates. The Privacy Shield introduced more structured commitments, requiring organizations to voluntarily commit to its Principles with the Department of Commerce, enforceable by regulatory authorities such as the FTC. This framework marked a shift towards greater accountability and public declaration of compliance.[134]

The DPF further solidifies this accountability and transparency, imposing additional layers of verification and ongoing compliance checks. Companies must not only adhere to the DPF Principles but also publicly commit to them, subjecting themselves to the enforcement powers of the FTC or the Department of Transportation. This commitment is not a one-time act; organizations are required to re-confirm their adherence annually, emphasizing a continuous commitment to data protection.[135]

In addition to the self-certification requirements, the new adequacy decision mandates organizations to engage in contracts for onward data transfers, extending the scope of accountability beyond the certifying organization to include their partners and service providers. This establishes a more interconnected and responsible data protection ecosystem.[136]

For organizations to certify under the DPF, they must first publicly declare their commitment to adhere to the EU-U.S. Data Privacy Framework Principles. This declaration involves implementing comprehensive privacy policies that embody these principles and making these

[134] Commission Implementing Decision (EU) 2023/4745, 2.1.1.
[135] Commission Implementing Decision (EU) 2023/4745, 2.1.1.
[136] Commission Implementing Decision (EU) 2023/4745, 10

policies readily accessible to the public. The certification process requires organizations to submit detailed information to the Department of Commerce (DoC), including the organization's name, purposes for which personal data will be processed, types of personal data covered, and the verification method chosen. This submission also includes details about the independent recourse mechanism and the enforcement authority, ensuring that the organization falls under the jurisdiction of the FTC or DoT, which are crucial for the oversight and enforcement of compliance.[137]

The DoC plays a pivotal role in verifying that organizations meet all certification requirements, a step forward from the self-certification approach of Safe Harbor. This emphasizes the importance of active oversight and enforcement in ensuring compliance. The annual recertification requirement underlines the ongoing commitment of organizations to adhere to the principles, ensuring that organizations do not merely pay lip service to privacy standards but embed them into their operational practices.[138]

Moreover, the DPF enhances transparency and legal certainty by stipulating that organizations can only claim adherence to the principles after the DoC has reviewed and accepted their certification submission. This approach aims to prevent premature claims of compliance, addressing criticisms of previous frameworks. The public listing of certified organizations further enhances transparency, allowing stakeholders to easily identify organizations that are compliant with the DPF principles.[139]

In addressing the deficiencies of Safe Harbor and Privacy Shield, the DPF introduces a robust mechanism for certifying compliance, emphasizing transparency, accountability, and continuous adherence to its Principles. This evolution reflects a concerted effort to align with the GDPR's high standards and address the concerns raised by the Schrems cases, providing a stronger foundation for transatlantic data transfers in the digital age.[140]

This comprehensive approach to certifying compliance with the DPF, including annual recertifications, detailed submissions, and a commitment to transparency and enforcement, represents a significant shift in how data protection frameworks evolve to meet the challenges of the digital age. By building on the lessons learned from Safe Harbor and Privacy Shield, the DPF tries to set a new benchmark for international data transfer agreements, aiming to foster trust,

[137] Commission Implementing Decision (EU) 2023/4745, 2.3.1 (48); Annex III.
[138] Commission Implementing Decision (EU) 2023/4745, 2.3.1 (48-49)
[139] Commission Implementing Decision (EU) 2023/4745, sec. 49, 52, Annex III
[140] Commission Implementing Decision (EU) 2023/4745, Annex IV; 2.3.1 (48-52); 2.3.4 (59)

ensure legal certainty, and promote a culture of privacy that benefits individuals and organizations on both sides of the Atlantic.

7. Conclusion

The progression from Safe Harbor to the DPF underscores a significant enhancement in data protection standards and privacy principles, directly responding to the evolving digital landscape and societal expectations for privacy. The invalidation of Safe Harbor and subsequently Privacy Shield by the European Court of Justice in the Schrems I and Schrems II decisions highlighted critical inadequacies in U.S. data protection practices, particularly concerning governmental surveillance and data access.

- **Safe Harbor** was criticized for its inability to provide adequate protection against U.S. surveillance practices, lacking enforceable rights for EU citizens.
- **Privacy Shield** aimed to address these deficiencies by introducing more stringent data protection obligations for U.S. companies and ensuring better cooperation with European Data Protection Authorities (DPAs). Despite these improvements, it still fell short in protecting against U.S. surveillance, leading to its invalidation.
- **DPF** emerges as a response to these challenges, incorporating rigorous GDPR standards. It advances transparency and individual rights, introduces more secure enforcement mechanisms, and seeks to limit government access to personal data.

The comprehensive analysis presented throughout this thesis scrutinizes the evolution of transatlantic data protection frameworks, culminating in the Data Privacy Framework (DPF), within the intricate context of EU-U.S. relations, technological advancements, and the persistent challenge of U.S. surveillance practices. Through a detailed examination of the DPF's certification process, exceptions to adherence, shared enforcement responsibility, and potential challenges, the study foregrounds the nuanced attempt to reconcile the stringent data protection standards of the European Union with the U.S.'s approach to privacy and national security.

Key Findings and Implications:

- **Evolution and Consistency:** The transition from Safe Harbor to Privacy Shield, and now to the DPF, illustrates an enhancement of data protection measures, albeit with consistent underlying challenges related to U.S. surveillance practices. A critical assessment, as noted by Zweifel-Keegan, reveals minimal alterations between the Privacy Shield and the DPF, suggesting that approximately 90% of the content remains consistent, underscoring a

continuity rather than a radical departure in the U.S.'s approach to addressing EU concerns.[141]

- **Surveillance Laws and the Role of the DPRC:** The persistent inadequacies in U.S. surveillance law remain a pivotal concern, as highlighted by Max Schrems' critique of the DPF's effectiveness and the ambiguous use of terminology such as "proportionate" access by U.S. intelligence services. Despite the establishment of the Data Protection Review Court as a mechanism for judicial redress, its potential impact on U.S. surveillance practices is questioned, given its executive affiliation and the challenges it faces in meeting the CJEU's standards for independence and effective judicial protection.
- **Certification Process and Compliance:** The DPF introduces a rigorous certification process, emphasizing continuous adherence to data protection principles and annual recertification. This process, while aiming to enhance transparency and accountability, places significant obligations on self-certifying companies, which may find themselves constrained by the broader U.S. legal framework and unable to effectuate substantive change in surveillance practices.
- **Monitoring, Review, and Future Challenges:** The establishment of specific monitoring and review mechanisms under the DPF, including routine evaluations by the European Commission in collaboration with European DPAs and U.S. authorities, underscores an ongoing commitment to ensuring the framework's effectiveness. However, the potential for future legal challenges, as indicated by NOYB's intention to scrutinize the adequacy decision, suggests that Schrems III may indeed be a question of time.

Conclusion and Forward-Looking Considerations:

In light of these findings, it can be concluded that while the DPF represents a significant effort to address the complexities of transatlantic data transfers, its effectiveness is ultimately contingent upon substantive changes in U.S. surveillance law. The partial adequacy decision under the new framework, which deems self-certifying companies adequate based on their compliance with the DPF principles, reflects a pragmatic approach to enhancing data protection standards. However, the lingering concerns regarding U.S. surveillance practices, the ambiguous interpretations of key terms, and the structural challenges faced by enforcement mechanisms like the DPRC underscore the ongoing tensions between privacy rights and national security interests.

[141] C Zweifel-Keegan, 'Unofficial Redline (From PS to DPF Principles)' (International Association of Privacy Professionals December 2022) https://iapp.org/resources/article/redline-comparison-of-principles-privacy-shield-dpf/.

The majority of professionals from an EU perspectiveauthors are skeptical about the DPF's ability to meet EU legal standards. They argue that the broad definitions and objectives for data collection under U.S. law, along with the potential for presidential amendments or revocations of EO 14086, pose significant risks. They believe these factors could lead to the CJEU invalidating the DPF in a potential Schrems III case, as the framework may fail to ensure an adequate level of protection equivalent to EU standards.[142]

Some authors express doubts about the future of the DPF, recommending that companies consider it as a supplementary measure and continue using other compliance mechanisms to ensure robust data protection and compliance with GDPR requirements. Companies in the EEA may benefit from relying on DPF-certified US companies for data transfers but should be prepared to update DTIA documentation to reflect the latest legal developments.[143]

The forward-looking implications of this thesis suggest that achieving a fully adequate level of data protection that aligns with EU standards and withstands CJEU scrutiny requires not only procedural and regulatory adjustments under frameworks like the DPF but also fundamental legislative reforms in the U.S. surveillance regime. As the first review of the DPF is scheduled for July 2024, continuous monitoring, active engagement between EU and U.S. authorities, and an openness to adapt the framework in response to evolving legal, technological, and societal landscapes will be crucial.

In conclusion, while the DPF marks an important step forward in the quest for a resilient and effective transatlantic data protection mechanism, the journey towards reconciling the divergent privacy landscapes of the EU and the U.S. remains ongoing. The nuanced approach of the DPF, characterized by its detailed compliance obligations, enhanced enforcement mechanisms, and pragmatic handling of exceptions, sets a new benchmark for future frameworks. Nonetheless, the ultimate resolution of the underlying challenges will necessitate sustained dialogue, legal innovation, and a commitment to upholding the fundamental rights of individuals in an increasingly interconnected and data-driven world.

[142] Galehr, Stella, Transatlantic Data Transfers under the GDPR: Developments and Outlook (Zurich Open Repository and Archive, University of Zurich 2023) https://doi.org/10.5167/uzh-252334 accessed [16.05.2024]
[143] Determann L, Nebel M, and Schmidl M, 'The EU – US Data Privacy Framework and the Impact on Companies in the EEA and USA Compared to Other International Data Transfer Mechanisms' (2023) 6(2) Journal of Data Protection & Privacy 120

8. Bibliography

Legislation and EU Materials

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 [1995] OJ L281.
2. **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119.
3. **Commission Decision 2000/520/EC** of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215.
4. **Commission Implementing Decision (EU) 2016/1250** of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield [2016] OJ L207.
5. **Commission Implementing Decision (EU) 2023/4745** of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework [2023] OJ L207.

Articles and Online Resources

6. Kuner, Christopher, 'Art. 44' in **GDPR Commentary**.
7. Farrell, Henry, 'Negotiating Privacy Across Arenas: The EU-U.S. "Safe Harbor" Discussions' in Adrienne Héritier ed, **Common Goods: Reinventing European and International Governance** (2002) 101, 105-126.
8. Schwartz, Paul M., 'Privacy and Democracy in Cyberspace' (1999) 52 **Vand. L. Rev.** 1609.
9. Reidenberg, Joel R. & Francoise Gamet-Pol, 'The Fundamental Role of Privacy and Confidence in the Network' (1995) 30 **Wake Forest L. Rev.** 105, 113-14.

10. Bennett, Steven C, 'The "Right to be Forgotten": Reconciling EU and US Perspectives' (2012) 30(1) **Berkeley Journal of International Law** 161, 169.

11. Warren, Samuel D and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) **Harvard Law Review** 193.

12. Cohen, Neal, 'The Privacy Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework' (2015) 1 **Eur Data Prot L Rev** 240.

13. Savin, Andrej, 'EU-US Data Privacy Framework – The New Framework for Transatlantic Data Transfers' (2023) 4 **EuCML** 159.

14. Batlle, Sergi and van Waeyenberge, Arnaud, 'EU–US Data Privacy Framework: A First Legal Assessment' (2023) European Journal of Risk Regulation.

15. Gerke, Sara and Rezaeikhonakdar, Delaram, 'Privacy Shield 2.0 — A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States' (2023) 45(2) Cardozo Law Review (published February 2024).

16. Determann, L., Nebel, M., and Schmidl, M., 'The EU – US Data Privacy Framework and the Impact on Companies in the EEA and USA Compared to Other International Data Transfer Mechanisms' (2023) 6(2) Journal of Data Protection & Privacy 120.

17. Galehr, Stella, Transatlantic Data Transfers under the GDPR: Developments and Outlook (Zurich Open Repository and Archive, University of Zurich 2023) https://doi.org/10.5167/uzh-252334 accessed 16 May 2024.

Cases

18. Griswold v Connecticut (1965) 381 US 479.

19. Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

20. Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems [2020] ECLI:EU:C:2020:559.

Additional Online Documents and Reports

21. The White House, A Framework for Global Electronic Commerce. Available at: https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html [Last updated 1997].

22. European Data Protection Board, Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data under the EU-US Data Privacy Framework. Available at: https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [Accessed 3 April 2024].

23. European Parliament, 'Draft Motion for a Resolution' (LIBE Committee, RSP 2501, 2023). Available at: https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf [Accessed 02 April 2024].

24. European Parliament, 'Adequacy of the Protection Afforded By the EU-U.S. Data Privacy Framework' (P9_TA 0204, 2023). Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.pdf [Accessed 03 April 2024].

25. The White House, 'FACT SHEET: European Commission Announce Trans-Atlantic Data Privacy Framework' (25 March 2022). Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ [Accessed 04 April 2024].

26. Tony Romm, 'Amazon, Apple, Facebook and Google Grilled on Capitol Hill over Their Market Power' The Washington Post (29 July 2020). Available at: https://www.washingtonpost.com/technology/2020/07/29/apple-google-facebook-amazon-congress-hearing/.

27. European Data Protection Board, 'Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data under the EU-US Data Privacy Framework' (28 February 2023). Available at: https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [Accessed 3 April 2024].

28. Davinia Brennan, 'European Commission Publishes Draft Adequacy Decision for EU-US Data Transfers' (MATHESON, 15 December 2022). Available at: https://www.matheson.com/insights/detail/european-commission-publishes-draft-adequacy-decision-for-eu-us-data-transfers [Accessed 3 April 2024].

29. Rosa Barcelo, Romain Perray, David P Saunders & Simon Mortier, 'EU-US Transatlantic Data Flows Framework: EU Supervisors Shine Light at the End of the Tunnel' (MCDERMOTT WILL & EMERY, 9 March 2023). Available at: https://www.mwe.com/insights/eu-us-transatlantic-data-flows-framework-eu-supervisors-shine-light-at-the-end-of-the-tunnel [Accessed 3 April 2024].

30. U.S. Department of Commerce, 'Safe Harbor Overview' (2002). Available at: https://web.archive.org/web/20020601115555/www.export.gov/safeharbor/sh_overview.html [Accessed 13 May 2022].

31. Maximilian Schrems and noyb, 'European Commission gives EU-US data transfers third round at CJEU' (noyb.eu, 10 July 2023). Available at: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu [Accessed 10 July 2023].

32. The White House, 'Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities' (7 October 2022). Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ [Accessed 28 March 2024].

33. US Department of Justice, Regulation Creating the Data Protection Review Court (14 October 2022).

34. C Zweifel-Keegan, 'Unofficial Redline (From PS to DPF Principles)' (International Association of Privacy Professionals December 2022). Available at: https://iapp.org/resources/article/redline-comparison-of-principles-privacy-shield-dpf/.

Additional Cases and Legal Texts

35. Charter of Fundamental Rights of the European Union, art 52(1) [2000] OJ C364/01.

36. European Court of Human Rights (ECtHR), Klass and others v Germany, App no 5029/71 (6 September 1978).