DOI: 10.47743/eurint-2024-TUL • November 2024 • VOLUME 11

Third time's the charm? The EU – US data privacy framework

Bianca-Raluca Tulac ✉
Alexandru Ioan Cuza University of Iasi, Romania

Abstract: In the current context of globalisation, data transfer to non-EU countries is becoming an important component of international trade. For this reason, and by virtue of the right to the protection of personal data, the creation of a legal framework designed to provide adequate safeguards for European citizens is a constant concern of the European Union. Through the lens of this study, we aim to outline an overall perspective on the cooperation between the European Union and the United States of America, regarding the transfer of personal data. Starting from the exposition of the efforts made over time, in order to ensure a safety of the transatlantic flow of data, we will focus on the current provisions in force, known as "Privacy Shield 2.0", determining, at the same time, the possible practical implications of them. Therefore, based on the study of the new rules established by the Privacy Shield 2.0, we will draw out the basic principles applicable to the transfer of data to the United States, the concrete effects of this act, presenting the legal challenges that its adoption brings, but also the ways in which it influences the development of international trade. Last but not least, we will analyse the likelihood of an invalidation of Privacy Shield 2.0 by reference to the premises of a possible Schrems III case. In this respect, we will present, on the one hand, the criticism of the way in which the European Union and the United States have agreed to reform the agreement on the confidentiality of data transfers, and, on the other hand, the steps taken against it.

Keywords: personal data, personal data protection, GDPR, DPF, Schrems III case

Introduction

At a European level, the right of each person to the protection of their personal data is expressly enshrined in Article 16 paragraph 1 of the Treaty on the Functioning of the European Union, provisions that are corroborated with those in the Article 8 paragraph 1 of the Charter of Fundamental Rights of the European Union (CFREU). The object of this right, i.e., personal data, is defined in the light of Article 4 point 1 of Regulation (EU) 2016/679 (Regulation (EU) 2016/679), the main legal instrument regulating this matter.

✉ PhD Student at the Faculty of Law, Alexandru Ioan Cuza University of Iasi, Romania; e-mail: bianca.tulac18@gmail.com.

By virtue of this regulatory framework, personal data cannot be transferred outside the European Union unless an adequate level of protection is ensured. Under this aspect, Chapter IV article 25 Paragraph (1) of Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 (Directive 95/46/EC) provided that "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection".

Following the adoption of this act, the European Commission (EC), assessing the level of protection afforded to the transfer of personal data by third countries, found that the level of protection afforded by the United States (US) was insufficient (Câmpean, 2015).

In this context, the EU and the US have started negotiations on the creation of a framework to ensure an adequate level of protection for the transatlantic transfer of personal data. These negotiations resulted in the "Safe Harbor" system of principles in 2000. This system introduced a series of rules that had the role of facilitating the transfer of personal data of the European citizens, to be stored, analysed and used by the emerging services of the information society, such as social networks or services of provision of digital content (Katulić & Vojkovic, 2016).

However, these principles were invalidated in 2015 by the European Court of Justice (CJEU), by issuing a decision in the case of Schrems v Data Protection Commissioner (Case C-362/14), known globally as "Schrems I". This lack of success of "Safe Harbor" happened when Facebook Ireland violated Articles 7 and 8 of the Fundamental Charter of Human Rights by transferring personal data to US-based Facebook Inc. without providing an adequate level of protection. Thus, the US National Security Agency (NSA) obtained, through the PRISM program, unrestricted rights to intercept and research data (including personal data) held by the participants in the US Safe Harbor program, including Facebook (Vidovic, M. Š., 2015).

As a result of the invalidation of the Safe Harbor Principles, US companies processing personal data under them could no longer avail themselves of this framework but had to apply for a special authorization to transfer personal data from Europe. From a practical point of view, this meant higher costs, delays in transfers, and a reason to duplicate US data servers in the EU (Vidovic, 2015).

Given these negative consequences of invalidating the Safe Harbor principles, the EU and the US have resumed negotiations to establish a new legislative framework to regulate transatlantic transfers of personal data. Thus, on 12th July 2016 the EU-US Privacy Shield Agreement, also known in practice as "Privacy Shield 1.0", was adopted, which provided new standards to ensure the protection of the flow of personal data. However, it appears that this legislative instrument did not meet the requirements of the Directive 95/46/EC on ensuring

an adequate level of protection by the companies processing personal data. The CJEU, under review in the "Schrems 2" case (Case C-311/18), found that the provisions of US legislation in this area did not provide an adequate level of protection and were in breach of the GDPR.

Specifically, the Court pointed out that the mass surveillance of the transatlantic transfer of personal data under the Section 702 of the US Foreign Intelligence Surveillance Act (FISA), Executive Order 12333, and the Presidential Directive 28 allow access and use by authorities of personal data imported from the EU to the US and lack the necessary controls to adequately protect EU data subjects who may become the target of national security investigations (Sharp Cookie Advisors, 2020).

In addition to these shortcomings, the Court pointed out that the adequate level of protection of the data flow was also diminished by the fact that the authority established by Privacy Shield 1.0, in the form of an Ombudsman, which was competent to resolve complaints about improper processing of personal data by US companies, was not an independent one. Under this aspect, the Court observed the fact that the undersecretary of state conducting the investigation was an executive body, which did not have the authority to take coercive measures, and its decisions could not be challenged (Propp & Swire, 2020).

For these reasons, finding that although the US legislation has rules equivalent to those in the EU in the matter of personal data protection, they are not effective, by the Decision issued on July 16, 2020 in the case of Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Case C-311/18), the CJEU declared the Privacy Shield 1.0 invalid.

At the same time, through this decision, the CJEU confirmed that the Standard Contractual Clauses (SCC) was an appropriate mechanism to ensure transatlantic data transfer, with the mention that data operators or persons authorized by operators who rely on the Standard Contractual Clauses are obliged to verify if the legislation of the third country of destination ensures adequate protection, under the EU law, of the personal data transferred with the help of standard data protection clauses, providing, if necessary, additional safeguards to those provided by said clauses (OneTrust DataGuidance, 2022).

1. Privacy Shield 1.0

The pronouncement of the decision in the "Schrems II" case by the CJEU had the direct effect of creating a vacuum regarding the transfer of personal data from the EU to the US and required the resumption of negotiations in order to establish a new regulation in this field. The efforts made in this regard by the EU and the US have materialized through the adoption of an agreement implementing new rules applicable to the transatlantic transfer of personal data. Thus, on July 10th, 2023, the European Commission adopted the Decision on the adequacy of the level of data

protection for the EU-US Data Privacy Framework, according to a press release, a normative act known as "Privacy Shield 2.0".

Starting from outlining the context in which the Privacy Shield 2.0 was adopted and the ways in which the negotiations between the EU and the US took place, we will first clarify the notion of "adequate level of protection", in order to then list the additional guarantees introduced by the EC Decision.

1.1. General considerations on Privacy Shield 2.0.

The invalidation of Privacy Shield 1.0 did not mean an end to the transfer of personal data from the EU to the US, and the conditions under which they are regulated was no longer regulated by any rule, in December 2020, the EDPB (EDPB) developed a series of recommendations on the additional transfer mechanisms (EDPB, 2023a) to ensure that data flows between the EU and the US provided the necessary protection capacity. The EDPS has also provided additional guidance on data transfers by updating the Standard Contractual Clauses (hereandafter, SCCs) for data transfers, including clarifying what is meant by a "transfer" (Stewart & Scott, 2022).

During this time, the EU and the US collaborated in order to renew the framework applicable to these types of transfer, and following the commitments assumed by the US to adequately protect the personal data of European citizens, on April 6th, 2022, the EDPS published Statement 01/2022 on the announcement of an agreement in principle on a new transatlantic data privacy framework.

According to the statements made by the President of the European Commission, Ursula von der Leyen, and President Biden, on the occasion of the signing of this "agreement in principle," the framework will encourage transatlantic data flows, responding to the concerns expressed by the Court of Justice of the European Union in the Schrems II decision of July 2020 (EDPB, 2022).

The next step in the Privacy Shield 2.0 adoption process was the signing by President Biden of the Executive Order on Strengthening Safeguards for U.S. Electromagnetic Signal Intelligence Collection Activities (The White House, 2022), which outlines the implementation steps the U.S. government will take in advancing the EU-U.S. Data Privacy Framework (DPF) (Metcalf, C. P., 2022). This order was basically a way for the US to cement the commitments they assumed in March of 2022, with the signing of the "agreement in principle" previously mentioned.

By analysing the provisions of this order, signed on October 7th, 2022, we can see that they represent new guarantees introduced to ensure adequate protection of the transatlantic flow of personal data. In concrete terms, this Executive Order emphasized, in particular, the regulation of the remedies available to data subjects who are subject to unlawful processing of their personal data, namely the mass surveillance of personal data collection carried out under Section 702 of FISA, Executive Order 12333, and Presidential Directive 28. For this reason, these

additional safeguards can be said to have been implemented in the form of remedies against the shortcomings pointed out by the CJEU in Schrems II.

All these provisions of the Executive Order signed by President Biden on October 7 were the subject of a review by the European Parliament, which investigated whether the additional safeguards met the GDPR's requirements for an adequate level of protection for the transfer of personal data to third countries.

The result of this analysis was reflected in the European Parliament Resolution of May 11th, 2023, on the adequacy of protection offered by the EU-US DPF (European Parliament, 2023). Through this resolution, the European Parliament pointed out that the Executive Order adopted by the US to implement the EU-US Personal Data Privacy Framework fails to provide an adequate level of protection for the transfer of personal data in relation to the European framework, as the safeguards provided for therein are not sufficient (Bruder & Yaros, 2023).

Considering that through the Resolution of May 11th, 2023, the European Parliament formulated several criticisms regarding the effectiveness of the new guarantees and that the transatlantic data transfers carried out according to the Executive Order signed on October 7th, 2022, are not adequately protected, the European Commission continued negotiations with the US to modify the existing legislative framework and to strengthen guarantees in this regard.

Thus, on July 10th, 2023, the European Commission adopted the Decision on the adequacy of the level of protection for secure data flows between the EU and the US, according to which the US ensures an adequate level of protection, comparable to that of the European Union, for personal data transferred from the EU to US businesses under the new framework (European Commission, 2023).

This Decision marks the entry into force of the new transatlantic personal data transfer framework between the EU and the US, known as Privacy Shield 2.0.

1.2. What is an "adequate level of protection" for the transatlantic transfer of personal data?

As it is also clear from the description of the context of the adoption of the new EU-US personal data privacy framework, the main instrument under which Privacy Shield 2.0 entered into force was the Decision on the adequacy of the level of protection for secure data flows between the EU and the US.

Through this Decision, the EU has, practically, confirmed that the new borders introduced by this legislation provide an adequate level of protection for personal data being transferred across borders. In this situation, one may wonder what is meant by an "adequate level of protection".

Relevant in this sense are the CJEU's clarifications recorded in the Schrems I case, in which it ruled that "The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the

Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter (CJEU judgment in C-362/14, 2020).

Therefore, by referring to the terminology used by the EU, i.e., the notion of "adequate", we can see that adequacy implies the existence of measures guaranteeing the protection of personal data in an appropriate manner, similar to that conferred by the applicable EU legislation in this field.

1.3. DPF Principles

The architecture of the new Privacy Shield 2.0. has been designed with reference to a set of commonly recognized and applied privacy principles that align with the requirements of the GDPR. The purpose of these principles is to provide European citizens with the assurance that they benefit from the same protection mechanisms for their personal data even when transferred to the US.

According to a release from the Privacy Shield framework (2023), transatlantic transfers of personal data are governed by seven key principles and 16 additional principles. All of these principles are subject to a commitment that US companies adhering to the DPF must make in order to obtain certification by the US Department of Commerce (DoC) (Rabet, 2023).

The first privacy principle is the Notification principle, which requires a certified company to inform those whose personal data is covered by the DPF (DPF-covered individuals) to notify them of their rights and of the certified company's obligations under the DPF (Jacobson et al., 2024). As to when this information should be disclosed, this principle provides that notification should be made at the time of the collection of personal data or as soon as possible thereafter.

The second principle applicable to a transatlantic transfer of personal data is the principle of choice, under which certified companies are required to give individuals a choice as to whether their data will be disclosed to third parties or used for any purpose other than the purpose(s) for which it was originally collected (Barany Esq, S., 2023). In the case of sensitive information (i.e., information relating to medical or health conditions, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and sex life information), by applying this principle, the certified company must obtain the DPF data subject's "express affirmative consent" before disclosing the sensitive information to a third party or before using the sensitive information for a purpose not covered in the original notice or authorized by the express affirmative consent (Jacobson et al., 2024).

Under the principle of onward transfer liability, certified companies are obliged to transfer personal data to third parties only if they ensure that adequate

safeguards are in place to the same extent as they would have been without onward transfer (Barany Esq, 2023). To comply with this principle, from a practical point of view, the company processing the personal data must enter into a contract with the third party, which limits what the third party is allowed to do with the data and implements safeguards to protect the data after transfer (Barany Esq, S., 2023).

The Personal Data Security Principle refers to the obligation of certified companies to take measures to ensure that personal information is protected against loss, misuse, improper use, unauthorized access, alteration, or destruction (Stalla-Bourdillon, 2023).

In the same sense, the principle of data integrity and purpose limitation is also established, which means that personal data may only be used for the purposes for which it was collected or subsequently authorized by the person covered by the DPF while requiring reasonable steps to ensure the reliability of personal data in relation to its intended use, such as appropriate anonymization techniques for processing.

The sixth privacy principle is called the "access principle," which can be relied upon by persons whose personal data have been processed to access them. Specifically, this right allows people to correct, modify, or delete personal data that has been processed in violation of legal norms or that is inaccurate.

The last privacy principle is closely related to the new guarantee set up by Privacy Shield 2.0. to ensure an effective redress mechanism for resolving complaints against a possible breach of the right to the protection of personal data. Enshrined under the concepts of "redress", "enforcement" and "accountability", the principle places an obligation on certified companies to put in place mechanisms to provide redress for individuals affected by the non-compliant processing of personal data and to cooperate with the competent authorities in this matter.

1.4. The new safeguards on the transatlantic transfer of personal data introduced by Privacy Shield 2.0.

As mentioned above, when revising the personal data privacy framework, the EU and the US sought to respond to the observations made by the CJEU in the Schrems II case on the mechanisms that should ensure the protection of personal data transferred to a third state. In this context, the provisions of Privacy Shield 2.0., strongly influenced by the clarifications given by the CJEU, introduced those safeguards whose necessity resulted from the 2020 judgment.

First of all, one of the issues raised by the Court concerns the mass surveillance of the processing of personal data carried out under the provisions of Section 702 of FISA. It was reveled through the decision in the Schrems II case that such surveillance does not respect the principle of proportionality. This legislation therefore limits access by US intelligence services to the personal data of European citizens to what is necessary and proportionate to protect national security. In

practice, this provision is likely to minimize the processing of personal data and introduce the principles of proportionality and necessity specific to the GDPR.

Secondly, the Court criticized the fact that the Ombudsman responsible for resolving complaints regarding the illegal processing of personal data does not circumscribe the notion of "independent court" in the sense provided by the GDPR. Thus, through the lens of the new privacy shield, the EU and the US have also taken care to improve the complaint resolution mechanism by establishing an independent and impartial court to examine complaints related to the US activities in collecting information based on electromagnetic signals.

The former Ombudsman has been replaced by the Data Protection Review Court (DPRC), a data protection review court that independently investigates and resolves complaints, including by taking binding remedies, and even has the power to obtain relevant information from intelligence agencies or order the deletion of data processed in breach of the law (EC, 2023). Privacy Shield 2.0. has therefore provided European citizens with an independent and impartial redress mechanism for the collection and use of their data by US intelligence services (EC, 2023), which will enhance the protection of transatlantic transfers.

In order for the DPRC to meet the standards of impartiality and independence necessary to ensure adequate confidence in the complaint resolution process, it is envisaged that it will be composed of members from outside the US government. It is important to emphasize that these members are appointed on the basis of specific qualifications, can only be dismissed for just cause (such as a criminal conviction or being considered mentally or physically unfit to perform their duties), and cannot be instructed by the government (EC, 2023).

This additional warranty indirectly establishes a "dual degree of jurisdiction" in the matter of these types of claims. As the DPRC is the court of appeal against the outcome of a complaint, it will first be reviewed by the Civil Liberties Protection Officer in the Office of the Director of National Intelligence's Office (CLPO), a position created by Executive Order (OneTrust Data Guidance, 2023). In resolving complaints 'in the first instance', this body will issue binding decisions requiring any relevant agency or element of the US Intelligence Community ('IC element') to take appropriate remedial action (OneTrust Data Guidance, 2023). The outcome of this investigation will be communicated ex officio to the complainant, irrespective of whether or not his or her right to the protection of his or her personal data has been found to have been violated or whether the CLPO has issued a decision requiring appropriate remedies (OneTrust Data Guidance, 2023).

Following this notification, individuals who are dissatisfied with the decision taken by the Civil Liberties Officer may appeal to the DPRC. During the review procedure, each party will be assisted and represented by a lawyer specializing in this field who has extensive experience. Under this measure, Privacy Shield 2.0. introduces a guarantee of respect for the right to a fair trial, ensuring that the applicant's interests are properly represented and that the Court is well informed

about the factual and legal aspects of the case (EC, 2023). Similar to the completion of the first stage, the complainant will also be informed of the outcome of the review procedure by the DPRC.

If complainants do not wish to go through the above-described complaint resolution procedure, they may file a complaint directly with a DPF member organization, an independent dispute resolution body designated by that organization, national data protection authorities, the U.S. Department of Commerce, or the U.S. Federal Trade Commission (Filliatre, 2023).

In addition to all these possibilities, namely the recourse mechanism that European citizens can use when their personal data has been collected in violation of the applicable provisions, the Privacy Shield 2.0. provided for the establishment of an arbitration commission as the last possibility for the settlement of complaints. This panel will be composed of one or three arbitrators nominated by the disputing parties, who are chosen from a panel of at least ten arbitrators appointed by the US DoC and the Commission on the basis of their independence, integrity, and experience in US privacy law and Union data protection law (Filliatre, 2023).

The Privacy Shield 2.0. provided, as an additional safeguard for the protection of personal data, the possibility for the European Commission to periodically review the EU-US data privacy framework in cooperation with representatives of the US authorities. In this respect, it was agreed that the first review will take place within one year of the entry into force of the adequacy decision. The purpose of this review is to verify that all relevant elements have been fully implemented in the US legal framework and are working effectively in practice (Bergt, 2023).

2. Practical implications of adopting Privacy Shield 2.0.

Transatlantic transfers of personal data are an important component of the global economy, with a volume exceeding that of any other international relationship and contributing to the $7.1 trillion US-EU economic partnership (Marconi, F., 2023). At the same time, more than 90% of EU businesses doing business with the US are involved in these data transfers, of which 70% are small and medium-sized enterprises.

In this context, the entry into force of Privacy Shield 2.0. has had a major practical impact, leading to a number of changes in the work of companies that process personal data.

2.1. Procedure for obtaining data controller certification

First of all, following the adoption of Privacy Shield 2.0., US legal entities that chose to adhere to its provisions can make transfers of personal data without the additional safeguards of protection required by the GDPR.

Joining the Privacy Shield 2.0. involves obtaining a "data controller" certification from the US Department of Commerce. Specifically, the procedure for US companies to obtain this certification differs depending on whether or not they have previously joined Privacy Shield 1.0. But regardless, all companies seeking to become certified must first submit few information to the Department of Commerce (DoC) through the DPF website, such as the name of their organization and a description of the purposes for which they process personal data (Burton et al., 2023).

If a company has already been certified as a data controller with the adoption of Privacy Shield 1.0, it must update its privacy policies in line with the new principles introduced by Privacy Shield 2.0. However, just updating is not enough; they are required to get DoC's approval to be added to the list of DPF participants, and to maintain their certification, they must pay a fee and recertify their privacy policy annually (Burton et al., 2023).

On the other hand, if a company wants to join such a regulatory framework for the first time, it must first meet the eligibility requirements, i.e., it must be a US legal entity under the control of the Federal Trade Commission (FTC) or the US Department of Transportation (Miño, 2023). However, telecommunications companies, most banking institutions, trade unions, most non-profit organizations, or most companies involved in packaging and storage activities are not eligible to obtain data controller certification (Miño, 2023).

Once a U.S. company meets the eligibility requirements, it must adhere itself to a set of privacy obligations that originate from those under the U.S. Privacy Shield and are similar to the GDPR's core principles (Everett & Wiseman, C., 2023). Assuming these obligations implies, at a practical level, taking measures to ensure that the company's activities comply with the principles of confidentiality.

A first step for the US company is to revise or adopt a privacy policy regulating the transatlantic transfer of personal data internally.

As mentioned above, one of the new safeguards introduced by Privacy Shield 2.0. concerns the provision of an effective complaint redress mechanism against unlawful processing of personal data. Therefore, in order to respect this guarantee, US companies seeking certification must provide access to an independent court to resolve complaints. . In concrete terms, fulfilling this obligation requires the registration of the company with a specific redress mechanism, which can be achieved through its voluntary commitment to the jurisdiction of EU data protection authorities, including through independent alternative dispute resolution or privacy programs developed by the private sector (Everett & Wiseman, 2023).

Since Privacy Shield 2.0. also provides for an arbitration of disputes that arise from the transfer of personal data, in order to obtain certification, US companies are required to contribute to the arbitration fund, which is used to pay the costs of the arbitration, including the arbitrators' fees, up to a maximum amount (Data Privacy Program, 2023). These fees must be paid before the U.S. Department of Commerce's

International Trade Administration (ITA) finalizes the certification (Data Privacy Program, 2023).

Last but not least, US companies need to put in place their own regular compliance verification mechanism, which can be done either by appointing an internal DPF compliance contact person (Fournier, 2023) i.e., self-verification, or by an external body (Thomas, 2023).

The finalization of the certification procedure takes place when the American company is listed by the ITA under the Data Privacy Framework. However, this certification is only temporary and valid for one year (Naumchuk, A., 2024). Therefore, at the end of this time, if a company wishes to extend its DPF certification for another year, it must recertify under the DPF program and demonstrate continued compliance with the DPF principles (Naumchuk, 2024).

2.2. Practical implications for US companies that do not want to join Privacy Shield 2.0.

If a US company previously adhered to Privacy Shield 1.0 but is unwilling to revise its privacy policy to align with Privacy Shield 2.0 principles, then it has the option to opt out of the framework.

To do so, the company must notify the DoC in advance and complete a withdrawal form available online. Upon registration of this request, the ITA will remove the company from the Data Privacy Framework List and add it to the authorized registration of U.S. organizations that have previously self-certified with the ITA but have been removed from the Data Privacy Framework List (Data Privacy Program, 2023).

Also, following this removal from the Data Privacy Framework List, the company must delete or return the personal data collected (Braun et al., 2023). However, the company has the option to retain the data already collected, provided that it declares annually to the Department of Defense, through its annual recertification, its commitment to continue to apply the principles or to provide adequate protection of personal data by other authorized means, such as standard contractual clauses (Braun et al., 2023).

We remind you that joining Privacy Shield 2.0. offers US companies the benefit of collecting personal data from EU territory without presenting additional safeguards. *Per a contrario*, in the absence of certification under the GDPR, companies will have to put in place their own safeguards to protect the transatlantic transfer of personal data in order to comply with the GDPR.

One such common mechanism in the practice of transatlantic transfers of personal data is the standard contractual clause (SCC). "According to the General Data Protection Regulation (GDPR), contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses – the so-called standard contractual

clauses (SCCs) – that have been "pre-approved" by the European Commission" (EC, 2022).

Another alternative to standard contractual clauses is the use of binding Corporate rules (BCR). However, this personal data protection mechanism can only be used for intra-group transfers in accordance with Art. 47 of the GDPR (Determann & Nebel, 2023). "BCRs require the approval of the data protection authority, which generally cooperates through the consistency mechanism pursuant to Article 63 of the GDPR. If the competent data
protection authority approves the BCRs, the other authorities in the EU are bound" (Determann & Nebel, 2023).

Thus, the use of the two alternative safeguards ensures that the requirements imposed by the EU under the GDPR for the adequate level of protection needed for transatlantic transfers of personal data are met.

3. The premises for invalidating Privacy Shield 2.0.

Ever since the new legal framework governing the transatlantic flow of personal data was adopted, there have been several criticisms about the effectiveness of the new safeguards it introduces. Therefore, in this section, we intend to analyze the premises of a possible invalidation of Privacy Shield 2.0 by referring, on the one hand, to the request of Mr. Philippe Latombe and, on the other hand, to the press releases of the non-profit organization None of Your Business (NOYB), led by Max Schrems, the supporter of the previous invalidations.

3.1. Application by Phillipe Latombe for the annulment and suspension of the DPF

On September 6th, 2023, Phillipe Latombe, member of the French Parliament and member of the Commission of the French Data Protection Authority (CNIL), submitted an application to the CJEU for the annulment of Articles 1 and 2 of the DPF request to, which was assigned the registration number T-553/53. However, it is important to emphasize that he did not make this request in his official capacity but as a European citizen, a user of Microsoft 365 and other applications, in which his personal data may be transferred to the US on the basis of DPF (Rennie, 2023).

In his request to annul the DPF, Philippe Latombe showed that this regulatory framework does not contain sufficient guarantees to ensure adequate protection of personal data in accordance with the GDPR. At the same time, through a press release, Latombe claimed that the DPF is the product of a flawed process of negotiation and consultation, the implementation of which did not respect certain procedural norms and which, ultimately, failed to adequately protect the fundamental rights of EU citizens (A&L Goodbody, 2023).

A first criticism made by Philippe Latombe is that the legislation is drafted only in English, which would contravene EU rules requiring regulations and other texts of general application to be drafted in the official languages (Defer, 2023). Subsequently, the DPF was published in the Official Journal of the EU in all official EU languages and can therefore be accessed by any EU citizen.

At the same time, Philippe Latombe considered that the DPF does not give European citizens access to an appeal that effectively ensures access to an impartial court. He argued that the US DPRC cannot be considered an independent court because it was created by presidential executive order and not by an act of Congress.

Last but not least, in his request to cancel the DPF, Philippe Latombe criticized the lack of transparency of the procedure for dealing with complaints submitted to the DPRC. In addition to the application for annulment of the DPF, Latombe also made a separate application asking the President of the CJEU to order a stay of execution of the adequacy decision (OneTrust DataGuidance, 2023). This request for suspension, however, was rejected by the CJEU, in an interim decision delivered on October 12th, 2023, on the grounds that Latombe had not demonstrated the urgency of the measure.

In the content of this rejection decision, the Court showed that the indispensable condition of urgency was not met because it couldn't be established whether the applicant would suffer serious damage if DPF wouldn't have been suspended. Analysing the grounds on which Latombe requested the suspension, the Court found that they were, in fact, too general and did not justify ordering this measure. In other words, they did not sufficiently set out, in his particular case, that transfers of his personal data, on a DPF basis, to a DPF-certified enterprise in the US would have caused him serious harm, especially given that, under certain conditions, transfers of personal data to the US were already permitted under the transfer instruments provided for in Articles 46 and 49 of the GDPR (Cavalier et al., 2023).

The court also noted that Philippe Latombe did not prove that he used certain IT tools (such as Microsoft 365, Google, and Doctolib) that would involve the transfer of his data to the US or that he could not use other protection mechanisms, such as standard contractual clauses or mandatory corporate rules, to ensure an adequate level of protection of his data (Richmond-Coggan & Eliyas, 2023).

In this context, the Court rejected his request without further examining the merits of the case or the balancing of interests, concluding that the mere demonstration of a prima facie case, even a particularly serious one, could not compensate for the lack of urgency (Richmond-Coggan & Eliyas, 2023).

On the other hand, with regard to the request for annulment of the DPF, the CJEU has not yet ruled on the merits of the case but is going to analyze whether the criticisms launched thereby are well-founded in such a way as to require the Privacy Shield 2.0 to be ineffective.

3.2. NOYB's intention to challenge Privacy Shield 2.0.

Maximillian Schrems, representative of the non-profit organization NOYB, announced on his website[1] his intention to challenge the new DPF.

In its release, Schrems pointed out, firstly, that although in the Schrems II case the CJEU found that the mass surveillance carried out under the Foreign Intelligence Surveillance Act Section 702 (FISA 702) was not proportionate within the meaning of Article 52 of the EU Charter of Fundamental Rights (CFR), the US has not taken steps to reform it.

The lack of an independent body to review the collection of personal data is another shortcoming of the DPF, according to NOYB. In this sense, it claims that the authority responsible for resolving complaints regarding the processing of personal data was only a partially independent executive body, which couldn't be considered an independent and effective court for the protection of the rights of data subjects. Based on these reasons, NOYB announced that it had already prepared several actions against DPF to bring it again before the CJEU. However, to date, none of these approaches have materialized.

4. Perspectives on the evolution of the EU – US DPF

In the context in which the regulation of data transfer involves a series of consequences, both on the political stage and at a practical level in the digital age, the adoption of Privacy Shield 2.0 raised a series of debates regarding the usefulness and impact of the new normative changes introduced by it. Thus, over time, specialized authors have critically analysed all these aspects and formulated various points of view regarding the possible future directions of EU-US relations in terms of data privacy.

Some authors have argued that this agreement between the EU and the US represents an important step in the evolution of international rules for the oversight of foreign intelligence services (Kerry, 2023). Contrary to those supported by Max Schrems, they appreciated that the changes introduced by this normative act are likely to strengthen the protection guarantees of the transfer of personal data (Kerry, 2023).

Moreover, they made some proposals to improve the system of protection for the transfer of personal data, pointing out that "passage of comprehensive commercial privacy legislation would help allay perceptions that the U.S. is the Wild West when it comes to data collection, even though that has not been at issue in the previous cases" (Kerry, 2023).

Privacy Shield 2.0. It also came under the scrutiny of a thorough analysis by the EDPB (EDPB), which on 28 February 2023 adopted Opinion 5/2023 regarding

[1] NOYB, retrieved from https://noyb.eu/en

the draft decision on the adequacy of the level of protection of the DPF (EDPB, 2023b),). With this opinion, the EDPB, while welcoming the changes to be implemented by this piece of legislation, also expressed concerns about the level of protection provided by the draft Adequacy Decision (Stassen, et al., 2023).

The EDPB's concerns were mainly related to the fact that although the safeguards to protect data transfers have been updated, they remained essentially the same as those set out in the previous privacy shields. In this respect, the EDPB takes into account both privacy principles and the remedies available to data subjects in the event of unlawful processing of their personal data.

The EDPB also made a number of recommendations in this opinion, suggesting the EC to clarify "the scope of exemptions, including on the applicable safeguards under U.S. law, in order to better identify their impact on data subjects. The Opinion also underlined that the European Commission should monitor the application and adoption of any statute or government regulation that would affect adherence to the DPF Principles" (Stassen et al., 2023).

It can be seen that these opinions have been drawn up following a comparative analysis between the new privacy shield and the previous ones. In other words, the specialized authors formulated assessments of the improvements brought by Privacy Shield 2.0., frequently referring to the provisions of the other agreements that were previously invalidated by the CJEU. Beyond criticizing the imperfections of the new measures to protect personal data transfers, they noted a substantial development in EU-US cooperation in this area.

Considering the particular importance of this new normative act, the EDPB did not remain passive; thus, establishing the strategy for the period 2024-2027, it adopted the Rules of Procedure (EDPB, 2024a), a public information note (EDPB, 2024b), and standard complaint forms (EDPB, 2024c) to facilitate implementation of appeal mechanisms under the DPF.

Moreover, in a statement published after the adoption of the new DPF, the EDPB President stated that "The adoption of the DPF by the European Commission, following the EDPB opinion of February 2023, is an important decision recognising that personal data can now flow from the European Economic Area to the United States, without any further conditions. It is essential that individuals are aware of their rights and that organisations know their obligations, which the EDPB explains in the information note. The EDPB will continue to pay special attention to the correct implementation of this new instrument and we look forward to contributing to the first review of the DPF next year" (EDPB, 2023c).

As we have stated in the lines of this article, one of the additional guarantees introduced by Privacy Shield 2.0. It implies its periodic review, precisely to correspond to everyday realities. Thus, on July 19, 2024, one year after the entry into force of the DPF, on the occasion of the first review, in a joint statement, the Commissioner for Justice and Consumers, Didier Reynders, and the US Secretary of Commerce, Gina Raimondo, underlined its practical effectiveness. In doing so, they

pointed out that, in addition to enhancing the privacy of European citizens in the US space, the DPF has facilitated flows of personal data underpinning EU-US trade and investment worth over 1 trillion dollars (EC, 2024).

However, some authors were of the opinion that its long-term success will depend on its ability to withstand legal challenges and adapt to evolving privacy standards (ComplexDiscovery, 2024).

On the other hand, in agreement with those supported by Max Schrems, other specialists believe that, despite the efforts made by both parties, the US policy does not meet the requirements of the adequate level of protection of personal data and that the Commission's decision on the adequacy of the level of protection presents crucial loopholes that ultimately allowed the EU to give the green light to an agreement that does not fully meet the EU's constitutional requirements (Boehm et al., 2024).

Therefore, given the different views on the evolution of the DPF, it can be said that although this regulatory framework has some shortcomings and can be improved, it is nevertheless viable, and attempts at EU and US cooperation in this area have not been without results.

However, the European Commission will prepare a forthcoming report on the occasion of the first annual review of the DPF, which will offer valuable insights into potential future directions of EU-US data privacy relations. For this reason, the discussions on this topic remain open, allowing the authors to articulate their vision and provide a more in-depth analysis of the long-term implications of this piece of legislation.

Conclusions

Transfers of personal data are one of the sectors whose importance in international trade cannot be denied, and the protection of personal data is a matter of concern for the participants in these operations. Although the Privacy Shield 2.0. has introduced additional safeguards for the transatlantic flow of personal data, unlike the previous protection mechanism invalidated by the CJEU, the criticisms raised suggest that these are insufficient to ensure adequate protection.

On a practical level, the likelihood of a Schrems III case before the CJEU is likely to cause confusion and uncertainty regarding the protection of data that are part of the transatlantic flow. Against this backdrop, from a practical point of view, the use by US companies of their own mechanisms to protect personal data, in particular standard contractual clauses, seems to be a more efficient method than the adherence to the DPF, which can be invalidated at any time.

Despite the uncertainties surrounding the adequate level of protection of the new DPF, the transfer of personal data is a reality today, which is why we appreciate that the existence of such a framework, which still providing a minimum level of protection, it is preferable compared to its absence.

References

A&L Goodboy. (2023, July 17). *EU-US Data Privacy Framework – at a glance*. https://www.algoodbody.com/insights-publications/eu-us-data-privacy-framework-at-a-glance

Barany Esq, S. (2023). *The EU-US Data Privacy Framework: What Is It and How Can My Organization Participate?* SixFifty. https://www.sixfifty.com/blog/eu-us-data-privacy-framework/

Bergt, J. (2023). *The EU-US Data Privacy Framework: A New Era of Transatlantic Data Protection*. Chambers and Partners. https://chambers.com/articles/the-eu-us-data-privacy-framework-a-new-era-of-transatlantic-data-protection-2

Boehm, F., Carrera, S., Mitsilegas, V., Pocze, J. (2024*). In the EU-US data transfer and privacy quarrel, the end is not in sight*. Centre for European Policy Studies. https://www.ceps.eu/the-eu-us-data-transfers-and-privacy-quarrel-the-end-is-not-in-sight/

Braun, M., Nahra, K. J., Pinto, T. Y., Mercer, S. T., Benizri, I., & Halim, V. (2023). *Certification Under the EU-U.S. Data Privacy Framework*. Wilmerhale. https://www.wilmerhale.com/insights/client-alerts/20230718-certification-under-the-eu-us-data-privacy-framework/

Bruder, A. H., & Yaros, O. (2023). *European Parliament adopts resolution about the draft US Adequacy Decision.* Mayer Brown. https://www.mayerbrown.com/en/insights/publications/2023/06/european-parliament-adopts-resolution-about-the-draft-us-adequacy-decision

Burton, C., De Boel, L., Padova, Y., Mithal, M., Kuner, C., Theodorakis N., Evans, T., Evrard, C., Nuding, M. (2023). EU and U.S. Finalize Data Privacy Framework: Here's How to Get Certified. *Wilson Sonsini*. https://www.wsgr.com/en/insights/eu-and-us-finalize-data-privacy-framework-heres-how-to-get-certified.html

Case C-362/14. Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362

Case C-311/18. Judgment of the Court (Grand Chamber) of 16 July 2020. Data Protection Commissioner/Facebook Ireland and Maximillian Schrems. https://curia.europa.eu/juris/document/document.jsf;jsessionid=EA3D06C518B95C5E0DB6DA401A07D4A6?text=&docid=228677&pageIndex=0&doclang=ro&mode=lst&dir=&occ=first&part=1&cid=1550817

Cavalier, M. (2023). EU-US Data Privacy Framework: No Urgency to Suspend, According to the CJEU. *Privacy World*. https://www.privacyworld.blog/2023/10/eu-us-data-privacy-framework-no-urgency-to-suspend-according-to-the-cje/

Câmpean, A. (2015). Un posibil semn că aplicabilitatea sistemului Safe Harbour se apropie de sfârșit. *Juridice*. https://www.juridice.ro/401832/un-posibil-semn-ca-aplicabilitatea-sistemului-safe-harbour-se-apropie-de-sfarsit.html

ComplexDiscovery Staff. (2024). *EU-U.S. Data Privacy Framework Under Scrutiny in First Annual Review*. https://complexdiscovery.com/eu-u-s-data-privacy-framework-under-scrutiny-in-first-annual-review/

Data Privacy Framework program (2024). *Withdrawal under the Data Privacy Framework (DPF) Program*. https://www.dataprivacyframework.gov/program-articles/Withdrawal-under-the-Data-Privacy-Framework-(DPF)-Program

Defer, A. (2023). *Il n'est pas urgent d'annuler le Data Privacy Framework qui lie l'UE et les Etats-Unis, selon la CJUE* [There is no urgent need to annul the Data Privacy Framework linking the EU and the United States, according to the CJEU]. L'Usine Digitale. https://www.usine-digitale.fr/article/non-il-n-est-pas-urgent-d-annuler-le-data-privacy-framework-qui-lie-l-ue-et-les-etats-unis.N2168837

Determann, L., & Nebel, M. (2023). The EU – US data privacy framework and the impact on companies in the EEA and USA compared to other international data transfer mechanisms. *Journal of Data Protection & Privacy*, *6*(2), 120-134.

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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

EDPB. (2022). *Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework*. https://www.edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf

EDPB. (2023a). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. https://www.edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

EDPB. (2023b). Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en

EDPB. (2023c). *EDPB informs stakeholders about the implications of the DPF and adopts a statement on the first review of the Japan adequacy decision*. https://www.edpb.europa.eu/news/news/2023/edpb-informs-stakeholders-about-implications-dpf-and-adopts-statement-first-review_en

EDPB. (2024a). *Rules of Procedure on the Data Protection Framework redress mechanism for national security purposes*. https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en

EDPB. (2024b). *Information Note on the Data Protection Framework redress mechanism for national security purposes*. https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en

EDPB. (2024c). *Template Complaint Form to the U.S. Office of the Director of National Intelligence's Civil Liberties Protection Officer (CLPO)*.

https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en

European Commission. (2023). *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows,* press relase. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

European Commission. (2023). *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

European Commission. (2023). *Questions & Answers: EU-U.S. Data Privacy Framework*. https://ec.europa.eu/commission/presscorner/detail/ro/QANDA_22_6045

European Commission. (2023). *Standard Contractual Clauses (SCC)*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

European Comission. (2024). *Joint Press Statement: Commissioner Didier Reynders and US Secretary of Commerce Gina Raimondo on the first periodic review of the EU-U.S. Data Privacy Framework*. https://commission.europa.eu/news/joint-press-statement-commissioner-didier-reynders-and-us-secretary-commerce-gina-raimondo-first-2024-07-19_en

European Parliament. (2023). *Adequacy of the protection afforded by the EU-U.S. Data Privacy Framework European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP))*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202301073

Filliatre, C. (2023). *European Union adopts a new framework for the transfer of personal data to the USA*. Soulier Avocats. https://www.soulier-avocats.com/en/european-union-adopts-a-new-framework-for-the-transfer-of-personal-data-to-the-usa/

Fournier, V. (2023). *10 FAQs about the New EU/US Data Privacy Framework*. OGC. https://www.outsidegc.com/blog/10-faqs-about-the-new-eu-us-data-privacy-framework

Jacobson, J. B., Kiosse, S., Friel, A., & Helleputte, C. (2024). *EU – U.S. Data Privacy Framework FAQs*. https://www.privacyworld.blog/data-privacy-framework-faq/

Katulić, T., & Vojković, G. (2016, May). From safe harbour to European data protection reform. In *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1447-1451). IEEE.

Kerry, C. (2023). *Will the New EU-U.S. Data Privacy Framework Pass CJEU Scrutiny?* Lawfare Media. https://www.lawfaremedia.org/article/will-the-new-eu-u.s.-data-privacy-framework-pass-cjeu-scrutiny

Marconi, F. (2023). *The EU–US Data Protection Framework: Balancing Economic, Security and Privacy Considerations.* Istituto Affari Internazionali. https://www.iai.it/en/pubblicazioni/eu-us-data-protection-framework-balancing-economic-security-and-privacy-considerations

Metcalf, C. P. (2022). *EU & US - The new EU-US Data Privacy Framework is finally here, or is it?* Linklaters. https://www.linklaters.com/en/insights/blogs/digilinks/2022/october/eu-and-us--the-new-eu-us-data-privacy-framework-is-finally-here

Miño, V. (2023). *What does the Data Privacy Framework Self-Certification mean for your company?* Datenschutz. https://www.datenschutz-notizen.de/what-does-the-data-privacy-framework-self-certification-mean-for-your-company-0545511/

Naumchuk, A. M. (2024). *How Should Companies Self-certify Under the EU-US Data Privacy Framework (DPF)?* Legal Nodes. https://legalnodes.com/article/data-privacy-framework-self-certification

OneTrust Data Guidance. (2022). *International: Overview of the DPRC Regulations.* https://www.dataguidance.com/opinion/international-overview-dprc-regulations

OneTrust Data Guidance. (2023). *EU: CJEU rejects request to suspend EU-US Data Privacy Framework*. https://www.dataguidance.com/news/eu-cjeu-rejects-request-suspend-eu-us-data-privacy

OneTrust DataGuidance. (2021). *The Definitive Guide to Schrems II*. https://www.dataguidance.com/resource/definitive-guide-schrems-ii

Privacy Shield framework (2023). *Arbitral Fund Contribution*. https://www.privacyshield.gov/ps/arbitral-fund-contribution

Propp, P., & Swire, P. (2020). *After Schrems II: A Proposal to Meet the Individual Redress Challenge*. Lawfare Media. https://www.lawfaremedia.org/article/after-schrems-ii-proposal-meet-individual-redress-challenge

Rabet, H. (2023). *Key Principles and Considerations for Participation in the EU-US Data Privacy Framework*. Katten. https://katten.com/key-principles-and-considerations-for-participation-in-the-eu-us-data-privacy-framework

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. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Rennie, P. (2023). *European court rejects EU-US Data Privacy Framework ("DPF") challenge*. Wiggin. https://www.wiggin.eu/insight/european-court-rejects-eu-us-data-privacy-framework-dpf-challenge/

Richmond-Coggan, W., & Eliyas, S. (2023). *EU-US Data Privacy Framework challenge rejected by EU General Court*. Freeths. https://www.freeths.co.uk/insights-events/legal-articles/2023/eu-us-data-privacy-framework-challenge-rejected-by-eu-general-court

Sharp Cookie Advisors. (2020). *Schrems II a summary – all you need to know*. https://www.gdprsummary.com/schrems-ii/

Stalla-Bourdillon, S. (2023). *What Is the EU-US Data Privacy Framework & How Should You Plan?* Immuta. https://www.immuta.com/blog/eu-us-data-privacy-framework

Stassen,M., & Sokova M., Crowell, Moring (2023). *EDPB's Opinion on EU-U.S. DPF*. Crowell. https://www.crowelldatalaw.com/2023/03/edpbs-opinion-on-eu-u-s-dpf

Stewart, K. E. S (2022). *EU and U.S. Reach Agreement in Principle on New Data Privacy*. Wiley. https://www.wiley.law/newsletter-April-2022-PIF-EU-and-US-Reach-Agreement-in-Principle-on-New-Data-Privacy-Framework-for-EU-US-Data-Transfers

Thomas, L. (2023). *Considerations for Participation in the EU-US Data Privacy Framework*. Sheppard Mullin. https://www.eyeonprivacy.com/2023/09/considerations-for-participation-in-the-eu-us-data-privacy-framework

Škrinjar Vidović, M. (2015). Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities. *Croatian Yearbook of European Law & Policy*, *11*(1), 259-276. https://hrcak.srce.hr/151459

White House (2022). *Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities