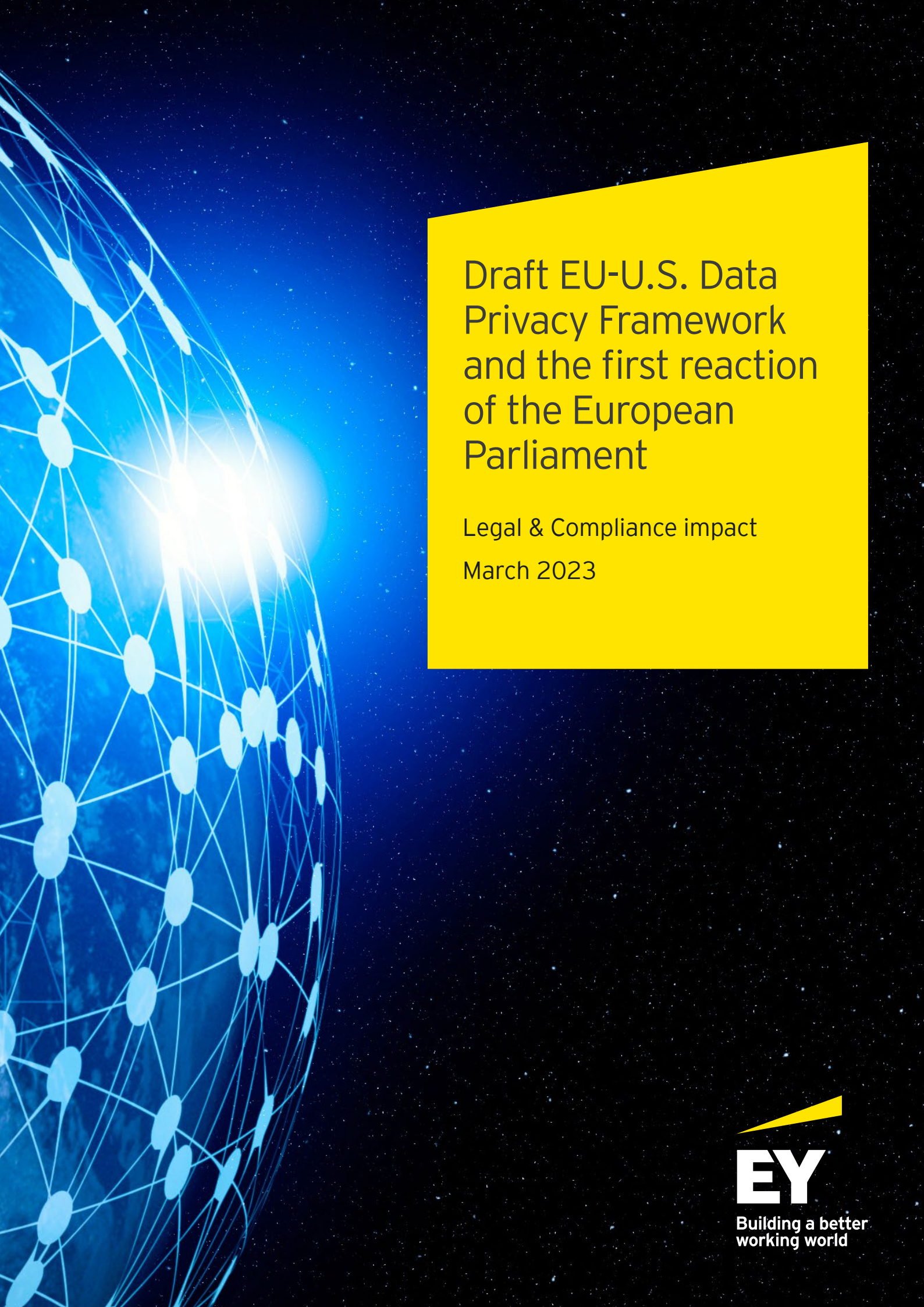


Draft EU-U.S. Data Privacy Framework and the first reaction of the European Parliament

Legal & Compliance impact

March 2023

Building a better working world

Executive Summary

After the invalidation of the Privacy Shield (Schrems II), the European Commission launched the process to adopt a new adequacy decision for data transfers between the EU and the U.S. resulting, in October 2022, in the draft EU-U.S. Data Privacy Framework (from here on: EU-U.S. DPF or DPF).

On 14 February 2023, the European Parliament already issued a draft motion for a resolution on the adequacy of this proposed draft EU-U.S. DPF. In short, the European Parliament concludes that the draft EU-U.S. DPF fails to create actual equivalence with the EU in the level of data protection that it provides.

Although it is a draft motion on a draft EU-U.S. DPF, we do see the Parliament exposes sensitive issues and topics that will not be put aside that easily since they relate to the essence of Schrems II.

We can expect the process of designing a final EU-U.S. Framework to take some more time. In the meantime, it is important to rely on the general regime applicable to transfers of personal data outside the EU without an adequacy decision:
(i) Know your transfer,
(ii) Verify your transfer tools,
(iii) Assess,
(iv) Identify and adopt supplementary measures,
(v) Re-evaluate.

Filip Bogaert
Partner
Legal

Table of contents

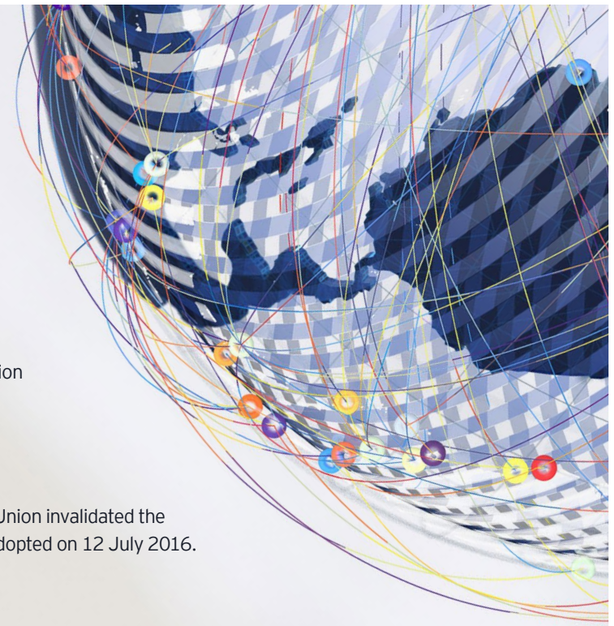
1 The EU-U.S. Data Privacy Framework

> Financial institutions transferring personal data outside the EU should make sure an adequate legal ground and, if necessary, sufficient mitigating measures are in place for each transfer.

Filip Bogaert
Partner
Legal & Regulatory

1.1 Context

Regulatory timeline: key dates



2016

12 July: The adequacy decision on the EU-U.S. Privacy Shield was adopted and allowed the free transfer of data to companies certified in the U.S. under the Privacy Shield.

2018

25 May: Entry into force of the GDPR (General Data Protection Regulation).

2020

16 July: Schrems II : The Court of Justice of the European Union invalidated the adequacy decision on the EU-U.S. Privacy Shield that was adopted on 12 July 2016.

2022

7 October: Signature of a U.S. Executive Order by President Biden along with the regulations issued by the U.S. Attorney General Merrick Garland.

12 December:

- Launch, by the European Commission, of the process towards the adoption of an adequacy decision for the EU-U.S. DPF ("Framework"),
- Publication of the draft adequacy decision,
- Transmission to the European Data Protection Board (EDPB) for its opinion (step 1 of adoption procedure).

2023

14 February: In a Draft Motion for a Resolution on the adequacy of the protection afforded by the proposed Framework, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs urged the European Commission not to adopt adequacy based on the Framework, on the basis that it "fails to create actual equivalence" with the EU in the level of data protection that it provides.

Next steps:

- The draft adequacy decision should go through its adoption procedure. This would require the following steps:
  - The Commission will seek approval from a committee composed of representatives of the EU Member States,
  - Once this procedure is completed, the Commission can adopt the final adequacy decision.
- However, given the negative Draft Motion of the European Parliament, we can expect renegotiations and redrafts to first take place before initiating the adoption procedure.

In 2020, by means of the so-called 'Schrems II case', the Court of Justice of the European Union (CJEU) declared invalid the "Privacy Shield" which allowed data transfer from the EU to U.S. companies, resulting in a legal and compliance issue for many EU-U.S. data transfers that were based on this Privacy shield: if no other legal ground was available, the transfer should be ceased immediately without a grace period.

The Privacy Shield was, inter alia, declared invalid due to a lack of protection of the personal data. The main reasons were:

- Shortcomings in the U.S. laws,
- No adequate protection against the far-reaching possibilities of surveillance,
- The fact that data subject rights were not actionable before the courts against U.S. authorities.

To tackle this, in March 2022, the European Commission and the U.S. announced an agreement on a new "Trans-Atlantic Data Privacy Framework" to be implemented by EU financial institutions wishing to transfer data to U.S. companies as well as regulate trans-Atlantic data flows. This agreement should address the concerns raised by CJEU in the Schrems II decision, and its purpose was to strengthen privacy and civil liberties protection from U.S. signals intelligence activities as well as to establish a mechanism with independent and binding authority.

Consequently, on 12 December 2022, the European Commission launched the process to adopt a new adequacy decision for the EU-U.S. DPF, which would try to address the concerns raised by the CJEU in its Schrems II decision.

The proposal for a draft adequacy decision follows the adoption of an Executive Order on 'Enhancing Safeguards for United States signals intelligence activities' by U.S. President Biden on 7 October 2022.

Although still being in a draft phase and before effectively coming into force, the further adoption process involves obtaining an opinion from the European Data Protection Board and the green light from a committee composed of representatives of EU Member States.

However, already before this process, on 14 February 2023, the European Parliament issued a draft motion for a resolution on the adequacy of the draft framework. In short, it concludes that the EU-U.S. DPF fails to create actual equivalence with the EU in the level of data protection that it provides. The Parliament calls on the Commission to continue negotiations with its U.S. counterparts in order to create a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU; which the European Parliament does not deem to be the case with the draft EU-U.S. DPF.

> "After the invalidation of the Privacy Shield, EU financial institutions should have ceased any transfer of personal data to the U.S. immediately if no other ground for the transfer was present.
>
> Filip Bogaert
> Partner
> Legal & Regulatory

1.2 Scope

Bearing in mind the historical context leading up to the EU-U.S. DPF (see above), it is also important to understand the legal setup and the content of the Framework. There are various legal grounds for transferring personal data outside the EU. These are adequacy decisions, binding corporate rules (BCRs), Standard Contractual Clauses (SCCs), Code of Conducts (CoCs), accredited third-party certifications and certain derogations (covered in art. 49 of the GDPR, such as consent, performance of a contract, ...).

- An adequacy decision is a formal decision made by the EU which recognizes that another country, territory, sector or international organization provides a level of protection for personal data equivalent to the one offered by the EU. The effect of such a decision is that personal data can flow from the Union to that third country without any further safeguards being necessary.
- The European Commission has so far recognized different countries as providing adequate protection, but these do not include the U.S.
- This adequacy decision on the EU-U.S. DPF would recognize that the U.S. ensures an adequate level of protection for personal data transferred from the EU to organizations certified under this Framework. It is important to understand that this adequacy decision is somewhat atypical compared to previous ones and relates only to organizations in the U.S. that are certified (see below) and not to the totality of the U.S. as a country.
- This also means that data transfers from the EU to entities not in scope of the EU-U.S. DPF cannot rely on this transfer mechanism, but are not automatically illegal or not compliant with the GDPR (see below).

A. Personal scope : Certified organizations

The EU-U.S. DPF is based on an adequacy decision for the U.S. but requires certification of each U.S. organization that wants to use it. The certification is completed by U.S. organizations committing to a set of privacy principles issued by the U.S. Department of Commerce (DoC). These are the 'EU-U.S. Data Privacy Framework Principles', including the Supplemental Principles: together they form the Principles.

To be eligible for certification under the EU-U.S. DPF an organization must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT). The Principles apply immediately upon certification.

EU-U.S. DPF organizations are required to re-certify their adherence to the Principles on an annual basis.

Certification is not mandatory. If an organization decides to be certified, it can use the adequacy decision. However, if an organization decides not to be certified, it is not necessarily prohibited to transfer personal data from the EU to that company. Indeed, those organizations will have to comply with another legal ground for transferring the personal data. To that end, the most used mechanism to transfer data from the EU are model clauses, which organizations can introduce in their commercial contracts.

B. Application process for certification

To certify under the EU-U.S. DPF (or re-certify on an annual basis), organizations are required to publicly declare their commitment to comply with the principles contained in the EU-U.S. DPF, make their privacy policies available and fully implement them.

To apply for such certification, organizations will have to provide the DoC with the following documentation :

- The name of the relevant organization,
- A description of the purposes for which the organization will process personal data,
- The personal data that will be covered by the certification, as well as the chosen verification method,
- The relevant independent recourse mechanism and the statutory body that has jurisdiction to enforce compliance with the Principles.

Organizations can receive personal data on the basis of the EU-U.S. DPF from the date they are placed on the DPF list by the DoC. To be allowed to continue to rely on the EU-U.S. DPF to receive personal data from the EU, such organizations must annually re-certify their participation in the Framework.

C. Material Scope : personal data shared from EU to U.S. certified organization

The protection afforded under the EU-U.S. DPF applies to any personal data transferred from the Union to organizations in the U.S. that have certified their adherence to the Principles with the U.S. DoC.

The covered personal data is defined in the same way as GDPR, i.e. as "data about an identified or identifiable individual that are within the scope of the GDPR received by an organization in the United States from the EU, and recorded in any form".

Accordingly, they also cover pseudonymized (or "key-coded") data, including when the key is not shared with the receiving U.S. organization. It is important to understand that only anonymized data is out of scope of the GDPR and most encryption tools and techniques only provide for pseudonymized data, which is still in scope.

- Pseudonymization: processing data in such a way that they can no longer be attributed to a specific person without the use of additional information like a coding key. This is e.g. the case for all encryption techniques that allow decrypting as well.
- Anonymization: processing data so that individuals are no longer identifiable from the data by anyone or any means. In this case, the data is e.g. encrypted irreversibly, so there is no key to go back to the original data.

1.3 Principles

The Principles provided in the DPF constitute a key component of the EU-U.S. DPF. They claim to provide organizations in the U.S. with a reliable mechanism for personal data transfers from the EU. These Principles should ensure that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to the U.S.

The Principles are intended to give comfort that the companies certified under the DPF receiving personal data from the EU would adhere to the DPF's standards.

There are **seven principles**:

- Notice,
- Choice,
- Accountability,
- Security,
- Data Integrity and Purpose Limitation,
- Access and Recourse,
- Enforcement and Liability.

However, those seven Principles under the draft EU-U.S. DPF are **exactly the same as the Principles that were applicable under the Privacy Shield**, which was declared invalid on account of invasive U.S. surveillance programs, thereby making transfers of personal data on the basis of the Privacy Shield illegal.

The question is thus whether or not this draft EU-U.S. DPF provides additional and sufficient guarantees that would make this proposal meet the constraints of the Schrems II case. Since the Principles (in this case: for certification) are exactly the same, the content seems to be rather weak. We therefore have a closer look into some additional safeguards the EU-U.S. DPF provides.

The EU-U.S. Data Privacy Framework

1.4 Proposed safeguards

A. Implementation of the certification – The DoC monitoring mission

The DoC would verify on an ongoing basis that the organization on the EU-U.S. DPF List effectively complies with the Principles.

As a part of its monitoring activities, the DoC would carry out "spot checks" of randomly selected organizations, as well as ad hoc "spot checks" of specific organizations when potential compliance issues are identified (e.g. reported to the DoC by third parties).

If there is credible evidence that an organization would not comply with its commitments under the EU-U.S. DPF (including if the DoC receives complaints or the organization does not respond satisfactorily to inquiries of the DoC), the DoC will require the organization to complete and submit a detailed questionnaire.

An organization that fails to satisfactorily and timely reply to this questionnaire will be **removed by the DoC from the DPF List and must return or delete the personal data received under the Framework**.

Furthermore, the DoC will send a notification to the contacts identified in the organization's self-certification submission specifying the reason for the removal and explaining that it must cease making any explicit or implicit claims that it participates in or complies with the EU-U.S. DPF and that it may receive personal data pursuant to the EU-U.S. DPF.

The notification, which may also include other content tailored to fit the reason for the removal, will indicate that organizations may be subject to enforcement action by the FTC, the DoC, or other relevant government body if they misrepresent their participation in or compliance with the EU-U.S. DPF, including in cases where they claim that they are participating in the EU-U.S. DPF after having been removed from the Data Privacy Framework List,

B. Enhancing Safeguards against United States signals intelligence activities

To enhance the safeguards against U.S. signal activities, which was one of the core reasons the Privacy Shield was declared invalid, the DPF inter alia foresees the establishment of the Data Protection Review Court (DPRC), which should provide protection for personal data with respect to government access for national security purposes.

This DPRC would aim at:

- Strengthening privacy and civil liberties safeguards to ensure that U.S. signals intelligence activities that take place are effectively necessary and proportionate in the pursuit of defined national security objectives,
- Establishing a new redress mechanism with "independent and binding" authority,
- Enhancing the existing rigorous and layered oversight of U.S. signals intelligence activities.

The aim of the provision of such a "court mechanism" would be that EU individuals may seek redress from a new multi-layer redress mechanism that includes an independent DPRC that would be composed of individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed.

> "Financial institutions should have a clear and ongoing view on their personal data processes and transfers in order to correctly assess Schrems II exposure and take the correct mitigating actions.
>
> Daan Thijs
> Senior Manager, Legal & Regulatory

2 | 14 February 2023: Draft motion for a resolution of the European Parliament

2. 1 Draft motion for a resolution of the European Parliament

On 14 February 2023 the European Parliament issued a draft motion for a resolution on the adequacy of the EU-U.S. DDPF – and this even before the EDPB was able to provide its opinion, which was the official first "next step".

The Parliament communicated a 'back to the drawing board' and had a rather negative opinion on the EU-U.S. DPF. The main reasons were the following (summarized in essence):

1 | It was pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the fundamental right to confidentiality of communication. This was indeed the essence of Schrems II.

2 | On the other hand, the Parliament acknowledged the efforts made in the Executive Order (EO) to lay down limits on U.S. signals intelligence activities by referring to the principles of proportionality and necessity, and providing a list of legitimate objectives for such activities. However, the Parliament also notices that:

- These principles are already long-standing key elements of the EU data protection regime and their substantive definitions in the EO are not in line with definition under EU law and their interpretation by the CJEU,
- For the purposes of the EU-U.S. DPF, these principles will be interpreted solely in light of U.S. law and legal traditions.

3 | The DPF still does not prohibit the bulk collection of data by signals intelligence, nor does it put limits or criteria on the content of communications subject to collection. Furthermore, the list of legitimate national security objectives (for signals intelligence) can be expanded by the U.S. President, who can even decide not to make the relevant updates public.

4 | There are concerns that the DPF does not apply to data accessed by public authorities via other means, for example through the U.S. Cloud Act or the U.S. Patriot Act, by commercial data purchases, or by voluntary data sharing agreements.

5 | Regarding the Data Protection Review Court (DPRC), a lot of weaknesses were pointed out that are not in line with EU expectations on adequate protection. This leads to the conclusion that the DPRC does not meet the standards of independence and impartiality as expected in the EU. The main reasons to come to that conclusion are:

- The DPRC's decisions will be classified and not made public or available to the complainant,
- The DPRC is part of the executive branch and not the judiciary,
- A complainant will be represented by a "special advocate" designated by the DPRC, for whom there is no requirement of independence,
- The redress process provided by the DPF is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data,
- The proposed redress process does not provide an avenue for appeal in a federal court and therefore does not provide any possibility for the complainant to claim damages.

6 | Lastly, the Parliament took the opportunity to point out that, unlike all other third countries that have received an adequacy decision under the GDPR, the U.S. still does not have a federal data protection law.

3 Conclusion

> Has your organization taken the necessary measures to implement the Schrems II judgement and be compliant in a future-proof manner?
>
> Filip Bogaert
> Partner, Legal & Regulatory

3.1 Conclusion

After the invalidation of the Privacy Shield (Schrems II), there was a legal and compliance issue for many EU-U.S. data transfers that were based on this Privacy Shield. If no other legal ground for the transfer was available, the transfer indeed needed to be ceased without a grace period. It goes without saying that the impact thereof is material.

This is obviously an undesirable situation: not only for the (legal and compliance) constraints, but also the uncertainty that companies need to deal with. The EU-U.S. DPF was drafted in an attempt to provide once again a legal framework by means of an adequacy decision for the EU-U.S. (personal) data transfers.

However, in order to be 'future-proof', it is of essence that the new Framework withstands the arguments that took down the Privacy Shield in the Schrems II case.

Unfortunately, it looks like the EU-U.S. DPF did not do so. As also noticed by the European Parliament the safeguards that should tackle the constraints of Schrems II seem unconvincing. There are not enough safeguards against access by intelligence authorities to the content of electronic communications and the DPRC does not meet the standards of independence and impartiality as expected in the EU.

Although it is indeed a draft motion on a draft EU-U.S. DPF, we do see that the Parliament exposes sensitive issues and topics that will not be put aside that easily since they relate to the essence of Schrems II.

We might expect the process of a (final?) EU-U.S. Framework to still take some time. Therefore, the current situation lacking an adequacy decision will probably remain for a while longer...

3.2 What should you do and how can we help ?

Given the recent draft opinion of the European Parliament, chances are unfortunately real that no solid equivalent for the Privacy Shield will be available in the very near future.

Therefore, one should (continue to) rely on the general regime applicable to transfers of personal data outside the EU without an adequacy decision, being;

- **(i) Know your transfer:** Map all your transfers of personal data to third countries; assess whether or not it is afforded an essentially equivalent level of protection wherever it is processed.
- **(ii) Verify your transfer tools:** If the transfer is based on an adequacy decision, monitor that decision. In case there is no adequacy decision (such as for the U.S.) you need to rely on other transfer tools, which are binding corporate rules, SCCs, approved code of conduct, approved certification mechanism, or in some cases rely on the derogations provided in article 49.
- **(iii) Assessment:** Assess if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer. Examine also the practices of the third country's public authorities, which will allow you to verify if the safeguards contained in the transfer tool can ensure a sufficient level of protection, or could be eroded by local authorities.
- **(iv) Identify and adopt supplementary measures:** This step is only necessary if your assessment reveals that the third country legislation and/or practices impinge on the effectiveness of the transfer tool you are relying on or you intend to rely on in the context of your transfer.
- **(v) Re-evaluate:** At appropriate intervals, assess the level of protection afforded to the personal data you transfer to third countries and to monitor if there have been or there will be any developments that may affect it. The principle of accountability requires continuous vigilance on the level of protection of personal data.

Your EY contacts

Filip Bogaert
Partner
Legal & Regulatory
filip.bogaert@be.ey.com
+32 477 631 462

Daan Thijs
Senior Manager,
Legal & Regulatory
daan.thijs@be.ey.com
+32 498 361 950

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY

EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com/be

EY is a leader in serving the financial services industry

We understand the importance of asking great questions. It's how you innovate, transform and achieve a better working world. One that benefits our clients, our people and our communities. Finance fuels our lives. No other sector can touch so many people or shape so many futures. That's why globally we employ 26,000 people who focus on financial services and nothing else. Our connected financial services teams are dedicated to providing assurance, tax, transaction and advisory services to the banking and capital markets, insurance, and wealth and asset management sectors. It's our global connectivity and local knowledge that ensures we deliver the insights and quality services to help build trust and confidence in the capital markets and in economies the world over. By connecting people with the right mix of knowledge and insight, we are able to ask great questions. The better the question. The better the answer. The better the world works.