EU-U.S. Data Privacy Framework: Current State and Possible Future Legal Challenges

October 20, 2025

Pittsburgh, PA

TEQ Hub

(by **Kristen Petrina**)

Due to the lack of a United States national data privacy law, the EU-U.S. have attempted to create a legal framework that permits a streamlined, regulated, and sufficient data transfer framework. Since 2015, three different data transfer agreements between the European Union and the United States were introduced. All three have faced challenges due to concerns the data transfer agreements did not provide adequate protections for EU citizens' data from U.S. government surveillance.

The first data transfer agreement implemented but was found to be inadequate and invalidated in 2015 by the EU's Court of Justice was the EU-U.S. Safe Harbor framework, which was deemed insufficient for protecting EU citizens' personal data and fundamental rights, particularly in light of revelations about U.S. surveillance programs. The second data transfer agreement implemented but ultimately found to be inadequate and invalidated in 2020 by the EU's Court of Justice was the EU-U.S. Privacy Shield framework, which was deemed to not offer the same level of protection as the GDPR. In particular, the framework did not adequately protect EU citizens' data from U.S. government surveillance. The EU-U.S. Safe Harbor and EU-U.S. Privacy Shield frameworks were challenged by Maximiliam "Max" Schrems and his data privacy rights organization NOYB – European Center for Digital Rights (NOYB). The challenges are referenced as Schrems I and Schrems II cases, respectively.

The third data transfer agreement implemented was the Data Privacy Framework (DPF). The EU-U.S. DPF was challenged by Latombe citing, among other claims, the U.S. Data Protection Review Court lacked true independence and impartiality, established as a key redress pillar under the DPF, and the sufficiency of safeguards governing bulk data collection by U.S. surveillance and intelligence agencies without prior authorization from EU citizens and lacked adequate oversight. The concerns were consistent with those raised in the Schrems I and Schrems II cases. Nevertheless, the European General Court dismissed Latombe's actions in its entirety, upholding the European Commission's adequacy decision.

The Latombe judicial challenge against the EU-U.S. Data Privacy Framework has been stopped by the European General Court. The ruling on September 3, 2025, conflicted with previously attempted EU-U.S. data transfer frameworks. The court dismissed the challenge brought by Philippe Latombe, Member of French Parliament (Latombe) to annul the DPF and reinforced the DPF's validity of the European Commission's adequacy determination for the U.S.

Data Privacy Framework

The most recent data transfer agreement between the EU-U.S. is the Data Privacy Framework (DPF). The DPF includes three different frameworks: (i) EU-U.S. Data Privacy Framework (EU-U.S. DPF), (ii) the UK Extension to the EU-U.S. Data Privacy Framework (UK Extension to the EU-U.S. DPF), and (iii) the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF). The DPF was developed to alleviate challenges faced by transatlantic commerce of U.S organizations. The DPF provides U.S. organizations with reliable mechanism that are consistent with EU, UK, and Swiss law for personal data transfers to the U.S. from the European EU (EU) and European Economic Area (EEA), the United Kingdom and Switzerland.

U.S. organizations participating in the EU-U.S. DPF may receive personal data from the EU/EEA in reliance on the EU-U.S. DPF after the European Commission issued the U.S. adequacy decision on July 10, 2023 ((EU) 2023/1795). The adequacy decision enables the transfer of EU personal data to participating organizations consistent with EU law. U.S. organizations participating in the UK Extension to the EU-U.S. DPF may receive personal data from the

United Kingdom and Gibraltar in reliance on the UK Extension to the EU-U.S. DPF. The data bridge for the UK Extension to the EU-U.S. DPF enables the transfer of UK and Gibraltar personal data to participating organizations consistent with UK law. Lastly, U.S. organizations participating in the Swiss-U.S. DPF may receive personal data from Switzerland in reliance on the Swiss-U.S. DPF, due to Switzerland's recognition of adequacy for the Swiss-U.S. DPF. The recognition of adequacy enables the transfer of Swiss personal data to participating organizations consistent with Swiss law.

U.S. organizations must self-certify to the International Trade Administration (ITA) within the U.S. Department of Commerce their compliance to each DPF framework. Organizations that only wish to self-certify and participate in the EU-U.S. DPF and/or the Swiss-U.S. DPF may do so; however, organizations that wish to participate in the UK Extension to the EU-U.S. DPF must participate in the EU-U.S. DPF. Once such an organization self-certifies to the ITA, the organization declares its commitment to the DPF Principles, that commitment is enforceable under U.S. law. Organizations participating in the DPF must annually re-certify. A U.S. organization's failure to re-certify, voluntarily withdrawal or determination by the ITA failure to comply with DPF requirements will result in removal from the DPF and must immediately cease claim of DPF participation. Nevertheless, upon removal from the DPF, U.S. organization's compliance with all DPF principles must continue for all personal information received while participating in the DPF for as long as it retains such information.

European General Court's DPF Legal Reasoning

- **Independence of the DPRC**

Latombe's primary argument and the cornerstone of the case was the structural dependence of the Data Protection Review Court (DPRC). The General Court reviewed the structure and function of the DPRC in detail, noting the appointment process for DPRC judges has multiple steps and layers, term limitations, and dismissal only for cause. Citing those findings, the General Court determined the judges were insulated from improper influence.

The General Court further discussed the statutory obligations on both the Attorney General and intelligence agencies, explicitly prohibiting their interference with the DPRC's work. Separately, the European Commission is required to continue to monitor the application of the DPF, and if necessary, suspect, amend or repeal the adequacy decision should changes in U.S. law or practice lessen the safeguards. These factors led the court to find that the DPRC met the EU standard of independent and impartial redress.

- **Bulk Collection and Proportionality**

The General Court reiterated that Schrems II did not demand ex ante judicial authorization, instead, it requires any bulk collection be subject to the meaningful, ex post judicial oversight. Separately, the General Court found that under U.S. law, collection of personal data by U.S. intelligence agencies is restricted to what is "necessary and proportionate" for clearly defined national-security purposes.

Further, such activities as bulk collection is subject to review DPRC, which has the authority to order remedial measures in cases where violations are identified. With this continued oversight, the General Court determined that the safeguards in the U.S. satisfy the "essential equivalence" test established by the Court of Justice of the European Union (CJEU).

Future of the DPF and Potential Additional Challenges

While this decision creates immediate stability for the DPF and participating U.S. organizations, the stability is not final.

Latombe has not indicated whether to expect an appeal, but he has until November 3, 2025 to decide whether to appeal the General Court decision to the CJEU. Separately, Max Schrems and NOYB issued a statement immediately upon the Latombe decision. NOYB argues that "*the lower court here massively departs from the case law of the CJEU…It may be that the General Court did not have sufficient evidence before it – or it wants to make a point to depart from the CJEU. We will have to analyse the ruling in more detail the next days*." NOYB is monitoring the Trump Administration Executive Orders, removal of 'independent' heads of organizations, indicating that the Latombe challenge as too narrow and a more expansive challenge may come. Therefore, it is unclear whether further judicial challenges will be raised, leaving the long term stability of the DPF in question.

Separately, beyond a Latombe appeal or an NOYB challenge, the European Commission is required to continuously monitor the U.S. for any significant changes, whether legislative or U.S. agency changes. Any changes that could be found to significantly vary from the current framework, could result in a partial or complete suspension of the adequacy decision.

Conclusion

While the Latombe decision provides clarity and current certainty for U.S. organizations that require EU-U.S. data transfers, it is crucial that U.S. companies continue to monitor the annual European Commission reports, possible Latombe appeal and other legal challenges that may be brough before the General Court of the CJEU. The landscape of data transfers, domestically and internationally continues to be dynamic, requiring ongoing monitoring and U.S. companies should remain cautious and vigilant to every occurring changes. Additionally, while the Latombe judgement was a win for the DPF, it does not eliminate the need for transfer impact assessments when using alternative transfer mechanisms, such as Standard Contractual Clauses, especially for U.S. data recipients who have not self-certified under the DPF.

To view the full article, **click here**.