BCLP. Client Intelligent

**Insights**

# THE EU-US DATA PRIVACY FRAMEWORK SURVIVES AN ANNULMENT CHALLENGE

Sep 08, 2025

SUMMARY

On 3 September 2025, the European Court of Justice ("CJEU") dismissed the action of a Member of the French Parliament, Mr. Philippe Latombe, who had sought annulment of the EU-U.S. Data Privacy Framework ("DPF"). Had he been successful, data transfers between the EU and US would have, yet again, faced challenges and uncertainty, as was the case following the 2020 Schrems II decision. This decision confirms that the European Commission is empowered to continue to review whether the DPF is sufficiently protective of EU data subjects' rights, as the US legal landscape evolves. However, at this time, the safeguards offered in the US for EU personal data have been deemed sufficient to ensure the DPF has weathered this annulment challenge.

## WHAT IS THE EU-U.S. DATA PRIVACY FRAMEWORK?

The EU-U.S. Data Privacy Framework is a legal mechanism governing the transfer of personal data from the EU to the US, adopted following the European Commission's adequacy decision of 10 July 2023. The DPF replaced the previous EU-US Privacy Shield invalidated by the (in)famous 2020 *CJEU Schrems II* ruling.

The DPF established a set of principles and commitments designed to ensure that US organizations that self-certify with the DPF and receive personal data from the European Union offer adequate protection for that data, comparable to the standards set out under the EU General Data Protection Regulation ("GDPR").

## WHY WAS THE DPF CHALLENGED BY PHILIPPE LATOMBE?

Mr. Philippe Latombe brought an annulment action under Article 263(4) of the Treaty on the Functioning of the European Union, which allows individuals to challenge EU acts that directly and individually concern them.

He raised a number of arguments that focused on the DPF's alleged failure to:

1. provide sufficient safeguards against government surveillance;
2. guarantee EU individuals access to an effective remedy before an independent tribunal, in spite of the establishment of the Data Protection Review Court ("DPRC"); and
3. offer sufficient protections to uphold the principles of proportionality and data minimization in data processing.

He also claimed that the DPF lacks a defined legal framework for automated decision-making (Article 22 GDPR), provides inadequate provisions regarding data security (Article 32 GDPR), and fails to comply with the EU's language requirements (Regulation No.1/1958). He argued that the DPF not only replicates the shortcomings of the Privacy Shield but also introduces new structural weaknesses.

## WHAT DID THE COURT DECIDE?

### INDEPENDENCE OF THE DPRC

The CJEU held that the DPRC does meet the standards of impartiality and autonomy needed for an independent tribunal, noting that its judges are appointed under strict criteria, are not part of the executive, and operate with full review powers (Recitals 44 and 51-59). The Court also rejected the claim that the DPRC was not "established by law" but created by executive regulation, emphasizing that sufficient guarantees were provided, including strict appointment and dismissal conditions (Recital 76), binding decisions (Recitals 76 and 78), and robust procedural safeguards such as panel composition and the role of a special advocate (Recital 77); and that pursuant to *Schrems II*, effective judicial protection may be provided by any body offering guarantees substantially equivalent to those required by EU law (Recital 81). Accordingly, this claim was rejected in its entirety.

### BULK COLLECTION OF PERSONAL DATA

Regarding the bulk collection of personal data by US intelligence agencies, the CJEU rejected the claim that such practices inherently violate EU law, clarifying that US law permits bulk collection only under strict conditions, with priority given to targeted methods and subject to post-collection judicial review by the DPRC (Recitals 107-116, 106). Instead, the CJEU reiterated that *ex post* judicial review suffices to meet the standards set by the *Schrems II* ruling. Ultimately, the CJEU found that the US system provides safeguards substantially equivalent to those required under EU law and rejected Mr. Latombe's argument.

## AUTOMATED DECISION-MAKING

Whilst the Court acknowledged that the DPF does not expressly cover the issue of automated decision-making (Recital 165), it emphasized that adequacy under Article 45 GDPR does not require identical safeguards to EU law, only a level of protection that is substantially equivalent (Recital 166). The Court noted US law provides relevant and effective safeguards in various economic areas, even if not as broadly framed as Article 22 GDPR (Recitals 175-177). The mere absence of a specific provision on automated decisions does not, in itself, undermine the overall adequacy of the DPF framework.

## SECURITY

The Court also dismissed the claim that the DPF did not comply with Article 32 GDPR requirements for data security obligations. Again, the CJEU held that adequacy does not require identical wording to EU law, but a framework offering substantially equivalent protection (Recitals 200-201).

Mr. Latombe's claim was therefore rejected and the validity of the DPF upheld by the CJEU. However, the CJEU reiterated the European Commission's role in monitoring its application in practice to ensure that the principles it contains continue to be effectively implemented in US law.

The Court also emphasized that "*the Commission is required to monitor continuously the application of the legal framework on which that decision is based*", and retains the power to "*suspend, amend or repeal the contested decision or to limit its scope*" should the US legal landscape evolve (CJEU Press release No.106/25). This decision reflects the dynamic nature of the DPF and the fact that its validity could be re-examined over time in light of its practical implementation, compliance challenges, administration of the certification regime, as well as future US legislative or political changes.

*Due to our footprint in Europe (UK, Germany and France) and in the United States and Middle East, the BCLP Global Data Privacy & Security team can assist you in developing your strategy for using personal data in the context of your transatlantic business.*

## RELATED CAPABILITIES

- Data Privacy & Security
- General Data Protection Regulation

## MEET THE TEAM

**Pierre-Emmanuel Froge**

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21

---