

JUNE 30, 2026 | PUBLICATION

Client Alert: U.S. Supreme Court Decision Prompts New Questions About EU-U.S. Data Transfers

EU-U.S. Data Transfers Remain in Effect Despite New Legal Questions

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

On June 29, 2026, the U.S. Supreme Court issued its decision in *Trump v. Slaughter*, a constitutional separation-of-powers case that has quickly generated discussion well beyond administrative law. While the Court did not address privacy or international data transfers directly, privacy advocates, including Max Schrems and the organization noyb (None of Your Business), argue that the ruling could have significant implications for the long-term viability of the EU-U.S. Data Privacy Framework (DPF).

Although some commentators have characterized the decision as fundamentally undermining the DPF, it is important to recognize that these conclusions represent legal arguments, not current legal determinations. At present, the European Commission's adequacy decision remains in effect, and organizations certified under the DPF may continue relying on it unless and until European institutions or courts take further action.

What Did the Supreme Court Decide?

In *Trump v. Slaughter*, the Supreme Court addressed the constitutional status of independent federal agencies and concluded that certain restrictions on presidential authority over executive officials are inconsistent with the Constitution. The decision specifically concerns the President's ability to supervise and remove officials serving in executive agencies, including the Federal Trade Commission (FTC).

The opinion does not discuss:

- The General Data Protection Regulation (GDPR);
- The EU-U.S. DPF;
- International data transfers; or
- The adequacy of U.S. privacy protections.

However, because the FTC plays a significant enforcement role within the DPF, the decision has prompted immediate debate among privacy practitioners regarding potential downstream effects.

Why Are Privacy Advocates Concerned?

noyb and Max Schrems argue that the ruling raises questions about whether the FTC can still satisfy the European Union's requirement that supervisory authorities exercising data protection oversight be sufficiently independent.

Their position rests on several arguments:

- The European Commission's 2023 adequacy decision repeatedly cites the FTC as an independent enforcement authority supporting U.S. privacy protections.
- EU constitutional provisions, including Article 16(2) of the Treaty on the Functioning of the European Union and Article 8 of the EU Charter of Fundamental Rights, require independent oversight of personal data protection.
- If the FTC is no longer considered sufficiently independent under EU law, Schrems argues that one of the factual assumptions underlying the adequacy decision has materially changed.

Based on that reasoning, noyb has formally requested that the European Commission begin an orderly withdrawal of the current DPF and has announced its intention to pursue additional litigation challenging the framework.

Important Context: The Framework Remains in Force

Despite the attention surrounding the decision, organizations should recognize several important legal realities: The DPF remains legally valid today, and the European Commission has not suspended or withdrawn its adequacy decision. Likewise:

- No court has invalidated the DPF;
- No European Data Protection Board (EDPB) guidance has instructed companies to stop relying on it; and
- U.S. companies certified under the DPF remain listed and eligible to receive covered transfers.

Accordingly, organizations relying on the DPF should continue monitoring developments rather than making immediate operational changes based solely on commentary or predictions.

Potential Future Developments

Several scenarios are now possible over the coming months and years:

European Commission Review

The Commission could determine that the Supreme Court decision does not materially affect the adequacy decision, or it could initiate a formal review to evaluate whether changes are necessary.

Judicial Challenge (Schrems III)

As with Schrems I (Safe Harbor) and Schrems II (Privacy Shield), a new challenge could eventually reach the Court of Justice of the European Union (CJEU). However, any such litigation would likely take years to resolve.

Additional U.S. Executive or Legislative Action

The United States could seek to strengthen aspects of the DPF through additional executive actions, agency restructuring, or congressional legislation designed to address European concerns.

Practical Considerations for Organizations

Organizations that transfer personal data between the EU and the United States do not necessarily need to change their compliance programs immediately. However, now is an appropriate time to review cross-border data transfer strategies and ensure contingency planning remains current.

Recommended steps include:

- Confirm which transfer mechanism your organization currently relies upon (DPF, Standard Contractual Clauses, Binding Corporate Rules, or Article 49 derogations).
- Review and update Transfer Impact Assessments where appropriate.
- Monitor guidance from the European Commission, the EDPB, and national supervisory authorities.
- Evaluate vendor contracts and identify alternative transfer mechanisms should the legal landscape change.
- Consider broader data localization or regional processing strategies where commercially feasible.

Organizations already using Standard Contractual Clauses should also recognize that future regulatory analysis could extend beyond the DPF, depending on how European regulators interpret the Court's reasoning.

Looking Ahead

The Supreme Court's decision has reopened an important conversation regarding the legal foundations of EU-U.S. data transfers, but it has not itself invalidated the DPF. Whether the ruling ultimately results in another major transatlantic privacy dispute remains uncertain and will depend on future actions by the European Commission and, potentially, CJEU.

For now, organizations should avoid reacting to headlines alone. Instead, they should continue monitoring developments, maintain documented transfer assessments, and ensure they are prepared should the regulatory landscape evolve.

For questions about the potential impact of this decision on your organization's cross-border data transfer practices, DPF compliance, or broader privacy obligations, please contact Jade Davis or another member of Shumaker Technology, Data Privacy, Cybersecurity & AI Service Line.

Sources

- *Trump v. Slaughter*, U.S. Supreme Court (June 29, 2026).
- European Commission Implementing Decision (EU) 2023/1795 on the EU-U.S. Data Privacy Framework.
- noyb (None of Your Business), "US Supreme Court just blew up EU-US Data Transfers" (June 29, 2026).
- Treaty on the Functioning of the European Union, Article 16.
- Charter of Fundamental Rights of the European Union, Article 8.

Editor's Note: This article is intended to summarize current legal developments and differing viewpoints within the privacy community. It does not express a position on the ultimate legal merits of the arguments raised and should not be construed as legal advice.

