Transatlantic Data Flows & the EU-US Data Privacy Framework

Consumers, Businesses, and Economic Growth Depend on Transatlantic Data Flows.

Companies of all sizes and in all industries need to move data across the Atlantic to reach customers, manage supply chains, collaborate on research, and improve the services they provide to businesses and individuals. And customers—on both sides of the Atlantic—deserve to know that their personal data will be maintained private and secure when their data is transferred. Transatlantic data flows are among the most important for both Europe and the US, accounting for over one-half of Europe's data transfers and about half of US data transfers.[1] Disruption to transatlantic data flows can have significant adverse effects on consumers, businesses, and economic vitality.

How Personal Data Is Transferred From the EU.

European Union law generally prohibits companies from transferring personal data from the EU to another country unless companies use an approved transfer mechanism. The approved transfer mechanisms are designed to ensure that EU fundamental rights are protected regardless of where the personal data is transferred. Currently, personal data can be transferred from the EU to another country through a determination by the European Commission that the other country's privacy protections are "adequate," or through Commission-approved commitments such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).

The EU-US Data Privacy Framework (DPF) Supports Transatlantic Data Transfers.

US President Joe Biden and European Commission President Ursula von der Leyen announced a political agreement on a new EU-US Data Privacy Framework (DPF) in March 2022.[2] It was implemented on July 10, 2023, after the European Commission issued a determination that commitments under the DPF create an "adequate" level of data protection.[3] The DPF creates a new mechanism to enable trusted data transfers while leveraging strong privacy standards. As a result, Companies can voluntarily certify to privacy principles recognized in the DPF, including specific business practices that respect privacy, to participate in the program.

---

1 Hamilton, Daniel S. and Joseph P. Quinlan, The Transatlantic Economy 2020: Annual Survey of Jobs, Trade and Investment between the United States and Europe (March 26, 2020), available at: https://transatlanticrelations.org/wp-content/uploads/2020/03/TE2020_Report_FINAL.pdf.

2 White House, Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (March 25, 2022), available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/; European Commission, Trans-Atlantic Data Privacy Framework (March 25, 2022), available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087.

3 European Commission, Implementing Decision of July 10, 2023, on the adequate level of protection of personal data under the EU-US Data Privacy Framework, available at https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

What Safeguards Are Included in the DPF?

The DPF provides a range of important protections for personal data transferred from the EU to the US under the agreement, including:

- New safeguards adopted by the US on its intelligence collection activities. These safeguards were implemented through an Executive Order.[4] They include ensuring that such activities take into account the privacy and civil liberties of all persons, regardless of nationality or country of residence, and be conducted only when necessary to advance a validated intelligence priority and only to the extent and in a manner proportionate to that priority.
- A new two-tier redress mechanism, established through the same Executive Order, for individuals to obtain independent and binding review and redress of claims about the collection and handling of their information. As part of that mechanism, a new Data Protection Review Court is created.

Importantly, the new safeguards on US intelligence collection and the new redress mechanism apply across transfer mechanisms. As a result, companies using SCCs, BCRs, other transfer mechanisms can rely on these protections.

Companies that participate in the DPF must also adhere to a range of privacy principles governing their own use and treatment of personal data received from the EU.[5] These DPF principles carry forward the substantive commercial privacy protections recognized by a prior transfer mechanism, the EU-US Privacy Shield Framework (Privacy Shield).

What Was the Privacy Shield? Why Was It Important?

The Privacy Shield was an important tool for transferring data between the US and EU, before it was invalidated by the European Court of Justice in the *Schrems II* decision in 2020. It was a voluntary program negotiated by the US Government and European Commission that allowed companies to self-certify to a set of privacy principles that ensure data is "adequately" protected when transferred to the US.[6] Over 5,200 organizations across a range of industries relied on the Privacy Shield to transfer data, more than 70% of which were small- or medium-sized businesses.

What Are SCCs? Why Are They Important?

SCCs are a vital, privacy protective mechanism used by millions of companies—European, American, and others—that transfer data in and out of Europe. SCCs impose a range of contract-based obligations on exporters and importers of personal data. These obligations—which are legally binding and fully enforceable under EU law—ensure that protections under the EU's General Data Protection Regulation (GDPR) apply to personal data transferred in accordance with the agreements. Today, SCCs underpin transfers of personal data from the EU not only to the US, but to over 180 countries—including Australia, Singapore, Brazil, India, and Mexico, among many others.

Consumers and Businesses Rely on Stable, Long-Term Mechanisms for Transatlantic Data Transfers.

The DPF provides a critical mechanism for responsible transatlantic data transfers, enabling the expansion of transatlantic commerce and strengthening data protection.

The DPF also reflects a recognition by the EU and US governments that protecting individual privacy and civil liberties is a shared goal. US and EU policymakers should continue working together on efforts that support reliable mechanisms for transatlantic data transfers, which can ensure that consumers have access to goods and services, businesses understand their obligations, and innovation and economic growth are uninhibited.

---

[4] Executive Order 14086 (October 7, 2022), available at: https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf. See also White House Fact Sheet (October 7, 2022), available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

[5] See Participation Requirements—Data Privacy Framework (DPF) Principles, available at https://www.dataprivacyframework.gov/s/article/Participation-Requirements-Data-Privacy-Framework-DPF-Principles-dpf.

[6] The Privacy Shield was a partial adequacy decision for companies under the authority of the US Federal Trade Commission.