Strengthening Transatlantic Data Flows

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 *Schrems II* Ruling Limited Organizations' Ability to Transfer Data.

The European Court of Justice (ECJ) considered the validity of the EU-US Privacy Shield Framework (Privacy Shield) and the use of SCCs to transfer data outside the EU in a decision issued in 2020. BSA participated as an amicus in the case, arguing that SCCs were intended to be used for transfers to countries that did not have an adequacy decision, and that a case-by-case decision must be made on whether their use provides sufficient protection.

On July 16, 2020, the ECJ invalidated the Privacy Shield as a mechanism for transferring data across the Atlantic in *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II).* It ruled, however, that SCCs remain a valid data transfer mechanism between the EU and US, though entities using SCCs (the exporter and the importer) are required to verify, on a case-by-case basis, whether the personal data can be provided the required privacy protection in the country where the data is transferred.

What Is the Privacy Shield? Why Is It Important?

The Privacy Shield was an important tool for transferring data between the US and EU, before its invalidation in *Schrems II*. The Privacy Shield 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

[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 (Mar. 26, 2020), available at: https://transatlanticrelations.org/wp-content/uploads/2020/03/TE2020_Report_FINAL.pdf.

data is "adequately" protected when transferred to the US.[2] 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 is the Trans-Atlantic Data Privacy Framework? What Will it Do?

On March 25, 2022, US President Joe Biden and European Commission President Ursula von der Leyen announced a political agreement on a new Trans-Atlantic Data Privacy Framework (Framework). The Framework will reestablish the Privacy Shield as a critical mechanism to enable trusted data transfers while leveraging strong privacy standards. Companies will once again be able to certify to the Privacy Shield, agreeing to specific business practices that respect privacy, and use it as a valid basis for EU-US data transfers after the new Framework is implemented. The new government commitments in the Framework are designed to provide appropriate protections from government access to data and recognize that those commitments must be implemented in a manner that effectively protects US citizens, and the citizens of US allies and partners, consistent with the high-standard protections created by the Framework.[3]

The Framework will also resolve any remaining questions about other transfer mechanisms, such as SCCs and BCRs, because the safeguards and government commitments in the Framework will apply across transfer mechanisms.

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 these 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. Without SCCs, companies around the world—both in and out of the EU—would have to curtail services significantly and customers would suffer as a result.

> According to a 2019 IAPP-EY report, approximately 88% of companies transferring data out of the EU rely on SCCs, while 60% used Privacy Shield.[4]

Consumers and Businesses Need Reliable, Long-Term Mechanisms for Transatlantic Data Transfers.

US and EU policymakers should continue working together on efforts that sustain 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.

The announcement of a new Framework is an important step in this work and reflects a recognition by the EU and US governments that protecting individual privacy and civil liberties is a shared goal. Indeed, the Framework can be an important pillar in the transatlantic relationship and set a powerful foundation for the important work of the US-EU Trade and Technology Council (TTC). Bringing the new Framework into force swiftly will enable expanded transatlantic commerce, strengthen data protection, and provide a reliable legal framework for responsible transatlantic data transfers.

---

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

[3] 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.

[4] IAPP-EY Annual Governance Report 2019 (Nov. 6, 2019), available at: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.