Trans-Atlantic Data Transfer 'Privacy Shield' Goes Live

July 15, 2016 Gavin George

RELATED PRACTICES Privacy and Cybersecurity, Technology Transactions, Intellectual Property

After two years of negotiations with the U.S. Department of Commerce, the European Commission this week finally adopted a new trans-Atlantic data transfer framework for U.S. businesses, known as Privacy Shield, that takes effect August 1, 2016. The negotiation process gained added urgency last October, when the EU Court of Justice struck down the previous 15-year-old Safe Harbor data transfer regime on the grounds that it failed to adequately protect the privacy rights of Europeans. The lack of a trans-Atlantic data transfer framework during the past nine months has been a key concern for global companies that rely on international data transfers and operate in the EU and the U.S.

As background, EU privacy law prohibits the transfer of personal data to U.S. organizations unless those organizations demonstrate an “adequate level of protection.” Until last year, the most common method to demonstrate this adequate level of protection was self-certification under the old Safe Harbor regime. The fallback method of demonstrating an adequate level of protection for European personal data, by adopting the EU standard privacy clauses into all trans-Atlantic contracts, tends to be more burdensome. As a result, U.S. businesses have been anxiously awaiting Privacy Shield to provide a convenient compliance mechanism following the demise of the Safe Harbor regime.

Unlike the previous Safe Harbor program, the new Privacy Shield framework requires U.S. companies processing European personal data to agree to comply with decisions by European regulators in relation to that data. Notably, Privacy Shield also requires companies to delete personal data that is no longer necessary for the original purposes for which they were gathered and processed.

The new Privacy Shield framework also allows Europeans to raise complaints about the mishandling of data in the U.S. through newly created channels, including a newly created privacy ombudsperson. The new framework also requires stronger monitoring and enforcement by the Department of Commerce and the Federal Trade Commission, which have both agreed to cooperate with European data protection authorities to investigate complaints.

There are also written safeguards and limitations in the new framework designed to prevent unrestricted access to bulk data transferred from Europe by U.S. law enforcement and intelligence agencies.

While the EU member states voted overwhelmingly in favor of Privacy Shield this week, the EU Parliament and EU data protection regulators have expressed concerns about its strength and legal adequacy. The new Privacy Shield framework will undoubtedly be subject to court challenges of the type that took down the Safe Harbor regime. If Privacy Shield is eventually struck down, companies should again be prepared to adopt the EU standard privacy clauses into their contracts and affiliate agreements as a fallback method or to include such clauses in all such newly entered or amended EU contracts.

© 2026 Haynes and Boone, LLP

The U.S. Department of Commerce will begin accepting self-certification applications to join Privacy Shield on August 1.

For additional information, please contact one of the Haynes Boone lawyers listed below.

© 2026 Haynes and Boone, LLP