

EU-US Data Privacy Framework: A New Era of the Transatlantic Data Transfer

July 14, 2023 Gavin George

PRACTICES Privacy and Cybersecurity, Intellectual Property

On July 10, 2023, the European Commission (EC) made an adequacy decision regarding the EU-U.S. Data Privacy Framework, marking a significant development almost three years after the Court of Justice of the European Union invalidated the previous EU-U.S. Privacy Shield Framework. The EC's decision holds that the United States provides a level of personal data protection that is equivalent to that of the EU. The decision paves the way for a reopening of the most direct corridor of personal data from the EU to the U.S. The U.S. companies participating in the new Data Privacy Framework will be able to avoid the hurdles of additional transfer safeguards (i.e. standard contractual clauses or binding corporate rules).

According to the EU Commission, the new Data Privacy Framework addresses all previous concerns raised by the EU's highest court, including with respect to access to EU data by U.S. intelligence services. The new Framework will be subject to periodic reviews by the EC and representatives of European data protection authorities and U.S. authorities.

To take advantage, U.S. companies must initially self-certify and then annually re-certify to the International Trade Administration (ITA) under the U.S. Department of Commerce that the company adheres to the Data Protection Framework "Principles." The certification process will remain substantially the same as those under the prior EU-U.S. Privacy Shield Framework, but the specific requirements are quite different.

U.S. Companies that have maintained their registration with the prior Privacy Shield Framework will be offered a simplified certification procedure. The U.S. Department of Commerce, which is charged with administering and monitoring the Data Privacy Framework has not shared very many details on the simplified procedure yet, but it has indicated that all participants are required to amend their privacy policies within three months.

Participants in the new Framework must offer an improved redress mechanism for assuring compliance with the Framework, and must provide recourse for individuals who are affected by alleged non-compliance with the Principles. Participants should plan to review and revise their internal processes and implement appropriate recourse mechanism.

After certification, companies must adhere to follow-up procedures for verifying that the attestations and assertions they make about their privacy practices are true and those privacy practices have been implemented properly in accordance with the Principles.

Additional details about the Data Privacy Framework and the certification process are expected to be posted on the U.S. Department of Commerce's dedicated website -- <https://www.dataprivacyframework.gov/s/>. According to the U.S. Department of Commerce, the website will be launched on July 17, 2023. At the same time, the old *privacyshield.gov* website will be shut down.

These new certification process and compliance will require all U.S. participants in the Framework to amend their privacy policies and review their existing data protection practices. If you have any questions, reach out to us at Haynes Boone LLP. Our privacy and data protection attorneys can help walk you through the Framework certification process.