Lowenstein Sandler

Privacy & Cybersecurity

October 18, 2022

The EU-U.S. Trans-Atlantic Data Privacy Framework Moves Closer to Approval: Why It Matters for Your Business

By Mary J. Hildebrand CIPP/US/E and Judith G. Rubin CIPP/US/E, CIPT

What You Need To Know:

- **On final approval, the EU-U.S. Trans-Atlantic Data Privacy Framework will replace the Privacy Shield, which was invalidated by the highest court in Europe in 2020.**
- **Under the new Privacy Framework, organizations that transfer personal data from the EU to the U.S. may obtain certifications from the U.S. Department of Commerce that the European Data Protection Board recognizes as providing "adequate security" for such data.**
- **There are several hurdles remaining before the new Privacy Framework is implemented, including review by the European Data Protection Board and approval by the EU member states, which could happen as early as 1Q 2023.**

An Executive Order to Reassure European Skeptics

President Biden recently signed the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities and supporting regulations (collectively, the "Executive Order"), enhancing privacy and civil rights safeguards for Europeans' personal data transferred to the U.S. The Executive Order represents significant progress on implementation of the EU-U.S. Data Privacy Framework (the "Privacy Framework") jointly announced by the United States and the European Commission in March 2022. The Privacy Framework is intended to replace the Privacy Shield, which was invalidated by the European Court of Justice (ECJ) in 2020 (the so-called Schrems II decision), primarily because the court determined that the U.S. does not provide "adequate security" for European personal data. There is a distinct possibility, although not any assurance, that the Privacy Framework will become effective early next year.

Why is the Privacy Framework needed?

The European Commission determined more than 20 years ago that only a relatively small number of the world's countries provide adequate security for the personal data of Europeans transferred into their jurisdiction. Despite a shared history and exceptionally close ties with the EU, the U.S. has never appeared on the approved list. Nonetheless, the volume of personal data transferred across the Atlantic, much of which is critical for business and commercial purposes, continues to increase (transatlantic data flows to the U.S. account for more than half of European data exports). EU organizations that export personal data and the U.S. recipients of that data are required to implement EU-approved safeguards for the transferred personal data described in the General Data Protection Regulation (GDPR), which included the Privacy Shield until 2020. By that point, more than 5,300 companies had been certified as Privacy Shield-compliant by the U.S. Department of Commerce.

What will the Trans-Atlantic Data Privacy Framework mean for businesses?

The Privacy Framework is intended to provide a durable and reliable legal basis for transatlantic data flows for organizations of all sizes and industry sectors. Based on the nature of companies that relied on the Privacy Shield for EU data transfer, small and midsize U.S. businesses may benefit the most. According to U.S. Commerce Secretary Gina Raimondo, the Privacy Framework "will enable the continued flow of data that underpins ***more than a trillion dollars in cross-border trade and investment every year*** and especially will benefit small- and medium-size enterprises, which make up 70% of the companies which will participate […]."

To achieve certification under the Privacy Framework, U.S. companies will be required to publicly commit to compliance with a comprehensive set of privacy principles and corresponding obligations and dispute resolution procedures that ensure EU residents have an opportunity to seek appropriate remedies for data misuse such as invasive activities by U.S. intelligence agencies. The U.S. Commerce Department will once again be responsible for administering the Privacy Framework, leveraging its Privacy Shield infrastructure and experience. After the Privacy Shield was invalidated, many U.S. companies elected to maintain Privacy Shield certification to indicate their continued commitment to data privacy, security, and regulatory compliance. While certification under the new regime is not automatic, the Privacy Framework currently does not include any radically different principles or obligations with respect to EU data transfer to the U.S. Even U.S. companies that currently rely on other GDPR-approved mechanisms may decide that, for certain data transfers, certifying to the Privacy Framework is preferable to the Standard Contractual Clauses, the Binding Corporate Rules, or the derogations under Article 49 of the GDPR.

When will the Privacy Framework be available to U.S. businesses?

There are several hurdles remaining until the final approval of the Privacy Framework. The European Commission is now turning its attention to preparing a draft adequacy decision based on U.S. assurances regarding EU personal data in the Executive Order. Next, the European Data Protection Board will review the draft and supporting materials and issue a nonbinding opinion, and the European Parliament may weigh in with a nonbinding resolution. Following these steps, the member states of the EU need to approve the draft. Once the draft is approved by the member states, the European Commission can adopt the final adequacy decision, which will be published in the Official Journal of the European Union and take immediate effect. Based on past proceedings of a similarly comprehensive nature, the ratification process may extend for about five to six months, which would mean that the Privacy Framework could be available to U.S. companies by March 2023.

Will the Privacy Framework last?

The Privacy Framework represents a concerted effort by U.S. and EU negotiators to solve for the concerns expressed by the ECJ in Schrems II regarding the protections for EU personal data afforded under the Privacy Shield. For this reason, the Executive Order provides additional safeguards that serve to limit access by U.S. national security authorities to EU personal data based on the principles of necessity and proportionality, and also establishes a new mechanism to provide remedies to EU residents. There should be no doubt, however, that the Privacy Framework will be challenged before the ECJ on similar grounds (and possibly by the same parties) after approval and implementation. Of course, the outcome is uncertain, but while the Privacy Framework is in effect, U.S. companies will enjoy a respite from the constant turmoil surrounding EU data transfer.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

JUDITH G. RUBIN CIPP/US/E, CIPT
Counsel
T: 212.419.5908
jrubin@lowenstein.com