Privacy Alert
July 2023

A Third Attempt at Adequacy: The EU-US Data Privacy Framework is Approved

The European Commission has adopted its adequacy decision regarding the EU-U.S. Data Privacy Framework (EU-U.S. DPF), agreeing that the United States offers an adequate level of protection—compared to that of the EU—for personal data transferred from the EU to U.S. companies participating in the EU-U.S. DPF. The decision grants companies the ability to transfer data of EU citizens to U.S. companies that have certified to the framework, without the need for additional authorizations. The adequacy decision follows the adoption by the U.S. of the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, which introduced new binding safeguards to address the issues raised by the Court of Justice of the European Union in the *Schrems II* decision. Among other things, the Executive Order establishes an independent and impartial redress mechanism to handle and resolve complaints from Europeans concerning the collection of their data for national security purposes.

Key Takeaways

- **1. Effective Immediately:** The framework allows for the immediate transfer of personal data between the EU and the U.S. without the need for additional safeguards such as Standard Contractual Clauses (SCCs). Companies that have been transferring data under the SCCs can rely on compliance with the framework to satisfy their transfer impact assessments.
- **2. Companies Will Need to Recertify:** Companies that maintained compliance with the Privacy Shield will need to update their certification and comply with a detailed set of privacy obligations and update their certifications. Additional guidance will be issued by the Department of Commerce's International Trade Administration.
- **3. Ongoing Oversight and Review:** The EU-U.S. Data Privacy Framework involves ongoing oversight and review to ensure compliance with data protection requirements. The U.S. Department of Commerce will monitor whether companies continue to meet the certification requirements, and the European Commission and representatives of European data protection authorities (DPAs) and U.S. authorities will also be reviewing the framework.
- **4. The Framework Will Likely Be Challenged:** Privacy advocacy organization NOYB (which previously challenged the Privacy Shield and its predecessor, the Safe Harbor Framework) has indicated that it intends to challenge the framework.

How Did We Get Here?

Under the General Data Protection Regulation (GDPR), personal data collected in the EU may only be transferred to a third country when the European Commission has decided that the third country ensures an adequate

Attorney Advertising

level of protection for that data. While the laws of the U.S. have not been deemed "adequate" by the European Commission, data has historically been transferred under data protection frameworks that have been deemed to provide an adequate level of protection.

The previous EU-U.S. data transfer framework, known as the Privacy Shield, was invalidated in July 2020 due to concerns about U.S. government surveillance practices and insufficient remedies for EU individuals. Following the invalidation, companies have relied on SCCs and Binding Corporate Rules (BCRs) to transfer data from the EU to the U.S.

EU-U.S. Data Privacy Framework Principles

The adequacy decision provides that the EU-U.S. DPF Principles apply immediately on certification. In addition, the Department of Commerce will provide a grace period of three months in which companies currently self-certified to the Privacy Shield can convert their self-certification to cover the DPF. The Department of Commerce will also provide a means for new companies to self-certify to the DPF. Companies will need to recertify their adherence on an annual basis, however. Under the framework, businesses will commit to a set of privacy principles issued by the Department of Commerce. These principles echo those in the GDPR, such as purpose limitation, data minimization and data security. EU citizens will gain rights including the right to access, rectify and delete data, as well as the right to object to the processing of data. Companies will also be restricted in further transfer of the data. Individuals who believe a business has failed to comply with their principles have redress options available through independent dispute resolution mechanisms and an arbitration panel. In order to ensure an adequate level of data protection, the Federal Trade Commission (FTC) and the Department of Trade (DoT), are tasked with monitoring and enforcing compliance with new rules.

The EU-U.S. DPF also includes safeguards that limit access to data to what is necessary and proportionate for national security, enhance oversight of intelligence activities and establish an independent redress mechanism. The Framework establishes a Data Protection Review Court (DPRC), to which EU individuals will have access, and introduces new redress mechanisms, such as giving the DPRC the ability to order the deletion of data collected in violation of the new safeguards. The DPRC will comprise members outside the U.S. government and will be supported by a special advocate to ensure fair representation and due process.

The Framework will be subject to periodic reviews, to be carried out by the European Commission together with representatives of European data protection authorities and competent U.S. authorities. The first review will take place within a year, in order to verify that all relevant elements have been fully implemented in the U.S. legal framework and are functioning effectively in practice.

Next Steps

The decision was entered into force on July 10 and is immediately effective. Companies interested in certifying under the privacy framework can take steps to participate and demonstrate their commitment to the obligations outlined in the decision. Specifically, companies will need to provide the following information to the Department of Commerce:

- A description of the activities whereby personal information of EU citizens would be received
- The business's privacy policy
- Contact information for handling complaints, requests or issues
- The statutory body that has jurisdiction to hear any claims against the business's privacy practices
- Privacy programs of which the business is a member
- Method of verification
- The relevant independent recourse mechanism for hearing privacy-related complaints

A simplified procedure for self-certification is available for companies that have previously self-certified under the Privacy Shield.

If a business is looking to transfer data of EU citizens but is not looking to certify under the Framework, alternatives for data transfer still include using SCCs or implementing BCRs.

Key Timelines

- July 10, 2023: The European Commission's adequacy decision for the EU-U.S. Data Privacy Framework entered into force. The EU-U.S. DPF Principles entered into effect as of the same date.
- July 17, 2023: The Data Privacy Framework program website (www.dataprivacyframework.gov) will go live. Businesses will be able to make initial self-certification submissions to participate in the EU-U.S. DPF and make annual recertification submissions.
- October 10, 2023: U.S.-based organizations that self-certified their commitment to comply with the EU-U.S. Privacy Shield Framework Principles must comply with the EU-U.S. DPF Principles, including by updating their privacy policies by this date.

Resources

- Press release
- Adequacy Decision
- Answers to FAQs
- DOJ Statement
- NOYB Statement

Related Professionals

Daniela Spencer . . . . . dspencer@loeb.com
Jessica B. Lee . . . . . jblee@loeb.com

7371 REV1 07-13-2023