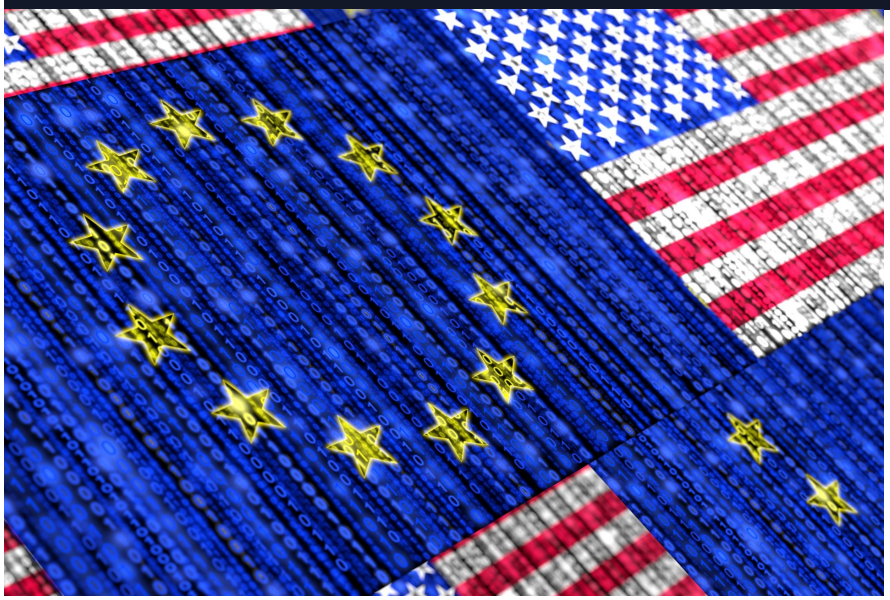
BARNES & THORNBURG LLP



ALERTS

European Commission Adopts Adequacy Decision For EU-U.S. Data Privacy Framework

July 24, 2023

Highlights

The United States has been deemed an “adequate” jurisdiction by the European Commission, allowing for a freer flow of transfers of personal data into the U.S.

The EU-U.S. Data Privacy Framework provides a number of important benefits to U.S.-based organizations and their partners in Europe

Businesses engaged in cross-border data transfers should consider taking steps now to self-certify to facilitate legally compliant transfers of data

After more than a year of negotiations between the U.S. and the EU, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework on July 10, 2023. The commission concluded that changes the U.S. agreed to adequately guarantee protection essentially equivalent to that guaranteed by the EU under laws like the General Data Protection Regulation (GDPR).

As a result, personal data may freely flow between the EU and U.S. for U.S. entities that agree to and certify their compliance with the framework.

RELATED PEOPLE

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

Maddie San Jose
Associate
Indianapolis

P 317-231-6416
F 317-231-7433
msanjose@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy
Intellectual Property

The framework, which includes the UK Extension and the Swiss-U.S. Data Privacy Framework, provides a number of important benefits to U.S.-based organizations, as well as their partners in Europe. It provides businesses a new opportunity to legally transfer personal data between the EU and U.S. that alleviates the need for alternate transfer mechanisms like the standard contractual clauses (SCCs).

Upon certification under the framework, businesses using the SCCs and other potentially unreliable transfer safeguards can shift to the framework as their primary method of data transfer. To establish viable transfers under the framework, businesses must complete a Data Privacy Framework Program self-certification process at dataprivacyframework.gov, update their privacy notice to include new framework language, and ensure all safeguards are up to date.

Joining the framework will further demand businesses revisit current data transfer agreements, review the transfer safeguards listed in current agreement templates, and work toward new agreements that encompass the framework's requirements.

Framework Adoption

The framework is considered an adequacy decision, a mechanism provided under the EU's GDPR that allows personal data to be transferred from the EU to a third country whose laws are deemed to provide adequate protection of personal data equal to that provided by the EU without requiring any further safeguards or authorizations.

The commission's adoption of its adequacy decision for the framework restores a reliable data transfer mechanism under EU law. Similar other mechanisms, namely the U.S.-EU Safe Harbor and the Privacy Shield, were invalidated by the EU Court of Justice on grounds that U.S. laws and government practices revealed by confidential documents released to the public by Edward Snowden showed that EU personal data was not protected in the U.S. by U.S. companies to the level required by EU laws. With the EU Court of Justice's Schrems II ruling in July 2020, the most popular alternative to the Privacy Shield, the SCCs became an unreliable means for most businesses to ensure the legal transfer of data. The SCCs were further called into question after a recent decision related to transfers by Meta Ireland.

On Oct. 7, 2022, President Joe Biden signed an executive order on Enhancing Safeguards for United States Signals Intelligence Activities directing the implementation of the framework and paving the way for the framework's adequacy decision. The executive order added binding safeguards to address the EU court's concerns with the previous mechanism. This and the subsequent regulation issued by the U.S. Attorney General in response formed the basis of the court's future adequacy decision on the framework, which entered into immediate force when adopted on July 10, 2023.

Framework Details

To achieve the adequacy decision and address concerns with previous transfer safeguards, the framework also agrees to limits on U.S. intelligence services' access to EU data. U.S. intelligence may now only

access EU data if it is deemed necessary and proportionate. The framework establishes a new two-layer redress mechanism to address disputes as to whether access meets this test. In addition to these limitations, the framework provides EU individuals with new rights to protect their data in the U.S. similar to rights granted under GDPR and U.S. data privacy laws, including the right to access, correct and delete their data under circumstances.

The framework is to be periodically reviewed by the European Commission, together with European and U.S. data protection authorities. The U.S. Department of Commerce administers and monitors the framework, and the U.S. Federal Trade Commission will enforce U.S. companies' compliance.

Compliance With the Framework

Companies must take certain actions to participate in the framework program and the benefits it provides. U.S. companies must self-certify their adherence to certain privacy obligations through the Data Privacy Framework Program website and publicly commit to comply with the framework's principles, which will typically be done in an online privacy policy.

When an organization initially self-certifies, it must include a draft privacy policy that complies with the framework principles. After a U.S. company self-certifies and publicly declares its commitment, its compliance becomes compulsory. Additional key requirements for compliance include publicly disclosing privacy policies, limiting personal information to what is relevant for the processing purposes, complying with the data retention provision, and informing individuals of their rights. Many of these requirements align with global privacy law principles.

To rely on the framework to legally protect data flows, organizations must be added to and remain on the Data Privacy Framework List, which the U.S. Department of Commerce's International Trade Administration (ITA) will update and maintain. The ITA provides guidance to companies seeking compliance. Participating companies must annually re-certify their compliance on the program website.

Steps to Comply

Organizations wishing to take advantage of the framework should consider following the steps to achieve certification:

1. **Eligibility**. An organization must confirm they are able to join the framework. Currently, "[o]nly U.S. legal entities subject to the jurisdiction of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DOT)" are eligible for participation.
2. **Contact**. The organization should designate an internal contact to handle all framework matters. This contact must be provided to the ITA and during the self-certification process.
3. **Privacy Shield**. If the organization previously committed to the outdated Privacy Shield, an organization that wishes to join the framework program is required to explicitly withdraw

from Privacy Shield and remove the commitment to Privacy Shield from its privacy policy.

4. **Privacy Policy**. Organizations must update their privacy policies to include a link to the U.S. Department of Commerce's Framework program website and a link or web address to the website or complaint submission form of the mechanisms available to investigate complaints. Once the privacy policy has been updated, an organization must send the draft to the ITA for its approval.
5. **Recourse Procedure**. Organizations must implement an internal recourse procedure to correct any compliance issues that arise, and ensure the organization has verification measures to verify that any privacy practices asserted in the new policy are true and in accordance with the framework.
6. **Policy Approval**. After the ITA approves the policy, companies should finalize and post the approved policy.
7. **Finalization**. After the approved policy is posted, organizations can submit the self-certification form. The ITA will then add the organization to the Data Privacy Framework List, and companies will be able to transfer their data under the framework.

Impact and Future Challenges

This adequacy decision is an important step toward securing valid legal transfers of personal data between EU and U.S. entities. It furthers EU-U.S. cooperation and allows businesses with operations in both the EU and U.S. to more easily facilitate necessary data transfers.

Because the framework's safeguards apply to all data transfers under the GDPR to participating companies in the U.S., regardless of the mechanism used, the adequacy decision currently provides more legal certainty than the SCCs or binding corporate rules. Organizations involved in frequent cross-border transfers should strongly consider acting to take advantage of the security and benefits offered under the framework.

Despite the positive impacts on businesses conducting international data transfers, the new framework is sure to bring legal challenges as did its predecessors. Max Schrems, a privacy advocate involved in legal challenges of EU-U.S. safeguard mechanisms, and the namesake of the well-known *Schrems I* and *Schrems II* decisions, immediately expressed shortcomings with the new framework, stating that the framework will be challenged and will not hold in the Court of Justice. Regardless of these potential challenges, businesses should consider taking full advantage of this new adequacy decision as perhaps the strongest mechanism currently available.

For more information, please contact the Barnes & Thornburg attorney with whom you work or Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com or Maddie San Jose at 317-231-6416 or msanjose@btlaw.com. This alert was drafted with the assistance of Hannah Kautz, summer associate.