Data Transfers Permitted Across the Pond via New EU-U.S. Data Privacy Framework

On July 10, 2023, the European Commission adopted its adequacy decision on data transfers for the EU-U.S. (European Union/United States) Data Privacy Framework (DPF). The adequacy decision concluded that the United States provides an adequate level of protection for personal data, with the implementation of this new framework. This landmark decision will be a welcome sea change for EU and U.S. companies, as those who participate in the DPF will be able to effectuate transatlantic data transfer safely and lawfully without need for additional transfer safeguards, including Standard Contractual Clauses (SCCs).

Adequacy Decision

Under the General Data Protection Regulation (GDPR), transfer of data outside of the European Economic Area (EEA) may only take place if the receiving country ensures an adequate level of data protection. The European Commission, pursuant to Article 45 of the GDPR, may designate certain non-EU countries as countries that provide an adequate level of data protection (adequacy decision) and if an adequacy decision is made relating to a specific country, data may be transferred freely outside of the EEA to that country without the requirement of any transfer mechanism. The adequacy decision on the DPF covers data transfers from any public or private entity in the EEA to US companies participating in the EU-U.S. Data Privacy Framework

Background

This decision comes nearly three years after the European Union's high court (Court Justice of the European Union or CJEU) struck down the EU-U.S. Privacy Shield Framework (See our previous articles on this subject for more information, *Restricted Data Flow: What US Businesses Need to Know about International Data Transfers in the Wake of Schrems II and the GDPR, High Court in the EU Strikes Down Privacy Shield*) and almost eight years after the CJEU declared the EU-U.S. Safe Harbor Framework invalid. Both frameworks were found to lack adequate protections from expansive U.S. governmental access to data or redress mechanisms for EU data subjects.

On March 25, 2022, the European Commission and the U.S. made an agreement in principle, outlining the U.S.' commitment to reforming its intelligence gathering surveillance practices. On Oct. 7, 2022, President Biden signed into effect an Executive Order called Enhancing Safeguards for United States Signals Intelligence Activities, which aimed to establish administrative safeguards to protect the legitimate privacy interests of individuals. The order was later supplemented by regulations issued by U.S. Attorney General Garland.

In December 2022, the Commission adopted a draft adequacy decision on the EU-U.S. Data Privacy Framework and on July 6, 2023, the EU comitology committee put forth a positive opinion of the decision, following vote with 24 out of 27 member states voting to approve the measure.

New Framework

While the new framework applies only to transatlantic data transfers made under the DPF, the adequacy decision will have implications in other areas of data transfer, as it reforms U.S. intelligence-gathering

wholistically. Under the adequacy decision, new rules and binding safeguards will be put into place to limit U.S. intelligence authorities' access to data based on necessary and proportionate principles to protect national security.

An organization that wants to make transfers under the DPF must self-certify with the U.S. Department of Commerce. This certification includes a commitment to adhere to certain principles including:

- Purpose Limitation and Choice: Personal data must be collected lawfully, fairly and for a specific purpose.
- Processing Special Categories of Data: The DPF places certain obligations on participants in relation to the collection and processing of special category data.
- Data Accuracy, Minimization, and Security: Organizations must take specific steps to ensure personal data is accurate, necessary for the purpose of processing, maintain in a secure manner provides protection against unauthorized or unlawful processing.
- Transparency: Data subjects must be informed of DPF organizations data processing activities including the purpose for processing, the parties that have access to personal information, and their individual rights, among other disclosures.
- Individual Rights: Data subjects must be informed of their rights in relation to processing of personal data and must be able to exercise those rights with participating organizations.
- Onward Transfers: DPF organizations will be responsible for any onward transfer of personal data and may need to implement certain contractual obligations with third parties receiving personal data.
- Accountability: As the DPF operates as a voluntary self-certification, organizations must implement appropriate technical and administrative measures to ensure compliance with the principles. Such measures include workforce training; internal policy and procedure creation; and outside compliance review. The DPF will likely replace the need for organizations to conduct Transfer Impact Assessments (TIA) previously used in EU-U.S. Data Transfers.

Organizations who choose to self-certify must comply with DPF principles and need to update privacy policies by Oct. 10, 2023.

Enforcement

A new two-tier redress system with specific monitoring and review mechanisms has been added for EU citizens who have concerns about the way their personal data is handled by U.S. Intelligence authorities. EU individuals will not need to demonstrate that their data was in fact collected by U.S. intelligence in order for their complaint to be admissible. In the new system, individuals can submit a complaint to their own national data protection authority, who will then transfer it to the United States and continue to provide updates to the individual on the progress of their complaint.

Under the two-tier system, complaints will first be investigated by the so-called 'Civil Liberties Protection Officer' of the U.S. intelligence community, who is responsible for ensuring compliance with regulations protecting privacy and fundamental rights. Second, if necessary, EU individuals may appeal the decision of the Civil Liberties Protection Officer to the newly created Data Protection Review Court (DPRC), composed of impartial members from outside the U.S. government. The DPRC is able to investigate these complaints, gather information from intelligence agencies, and make binding remedial decisions.

Limitations

Notably, the DPF only applies to organizations regulated by the Federal Trade Commission or the U.S. Department of Transportation. This means that nonprofit organizations will not be able to take advantage of the new framework and will likely have to continue relying on cumbersome SCCs. Further, the DPF only applies to transfers between the U.S. and the EU. While the United Kingdom (UK) is expected to follow suit, the DPF cannot currently be used to transfer data to from the UK. Finally, the DPF may be subject to legal challenges just like the Safe Harbor Framework and the Privacy Shield. The U.S. intelligence community's expansive powers still remain a concern for some European organizations, and we expect to see legal challenges to invalidate the DPF brought in the CJEU.

Key Takeaways

Organizations may self-certify their participation in the DPF by agreeing to comply with a detailed set of privacy obligations. Importantly, organizations that are already certified under the Privacy Shield framework will have access to a simplified procedure for self-certification under the EU-U.S. Privacy Shield Framework. These entities will likely be contacted by the U.S. Department of Commerce with regard to next steps for re-certification.

The EU-U.S. Data Privacy Framework will be subject to periodic reviews, with the first one taking place within a year of the enforcement of the adequacy decision to ensure effective functioning and compliance within the U.S. legal framework (sometime before July 10, 2024). As this is the third time the two parties have come to an agreement of this type, Bond will continue to monitor the adaptation and enforcement of the EU-US DPF for any updates to the framework or further recommendations for clients.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters including on matters regarding international data transfer and GDPR compliance. If you have any questions about cross-border data transfers or the EU-U.S. Data Privacy Framework, please contact Jessica Copeland, CIPP/US, Amber Lawyer, CIPP/US & CIPP/E, Mario Ayoub, or any attorney in Bond's cybersecurity and data privacy practice.

**Special thanks to Summer Law Clerk Haley Case for her assistance in the preparation of this blast. Haley is not yet admitted to practice law.*

BOND SCHOENECK & KING ATTORNEYS