Published on *The National Law Review* https://natlawreview.com

The New Privacy Shield – European Commission Adopts the EU-U.S. Data Privacy Framework

Article By:

On July 10, 2023, the European Commission (EC) adopted the European Union-United States Data Privacy Framework (DPF), an adequacy decision concluding that the U.S. has adequate data privacy and security infrastructure in place for secure transfer of personal data from the European Economic Area (EEA), which is comprised of the 27 European Union Member States, Norway, Iceland, and Liechtenstein, into the U.S. Prior to the adoption of the DPF, in order to transfer data from the EEA to the U.S., organizations in the U.S. were required to use one of the EC-approved safeguards, such as standard contractual clauses or binding corporate rules. These safeguards, set forth in Article 46 of the General Data Protection Regulation (GDPR), are onerous and complicated. The DPF allows for the safe and secure flow of data for U.S. multinational corporations and organizations doing business with those in the EEA. The importance of this data flow cannot be overstated – organizations across all sectors, whether large or small, will have equal opportunity to participate in the digital economy and to engage in streamlined international commerce.

There are three branches of the DPF – the EU-U.S. DPF, the Swiss-U.S. DPF, and the UK Extension to the EU-U.S. DPF. With the July adoption of the EU-U.S. DPF by the EC, the EU-U.S. DPF permits flow of information from the E.U. to the U.S. The Swiss-U.S. DPF and UK Extension to the EU-U.S. DPF will enable personal data transfers from those jurisdictions if and when the Swiss and UK Governments officially recognize the adequacy decision.

In the U.S., the DPF is implemented and administered by the U.S. Department of Commerce (DOC), and on July 17, 2023, the DOC launched the Data Privacy Framework program website. On this website, users can apply for their organization to participate in the DPF and be listed on the Data Privacy Framework List, the public record of all DPF participants that is published on the DPF Program website. Users may join the list via two methods: self-certification, or Outside Compliance Review. Organizations may self-certify that their organization meets the criteria set forth in the DPF and is committed to adhering to the principles of the DPF. The self-certification process requires users to provide basic information about the organization and contact information for someone within the organization who will handle complaints, access requests, and other issues concerning compliance with the DPF. Additionally, users must provide descriptions of:

- their organization’s activities with regard to all personal data received from the EEA;

- the independent recourse mechanism that will be used to investigate unresolved complaints; and

- a description of the organization's privacy policy, as well as a draft of the compliant policy.

Alternatively, organizations that do not wish to self-certify can opt to undergo an Outside Compliance Review by engaging a third-party that conducts such reviews, and providing the identity and website address of the third party. This is a good option for organizations that may lack the institutional knowledge and legal guidance required to self-certify. Most organizations will choose to self-certify; in fact, by 5:00 p.m. on July 17, 2023, over 260 organizations joined the Data Privacy Framework List by self-certifying.

If this all sounds familiar, that is because this is the third adequacy decision that has been adopted by the EC with regard to EU data transfers to the U.S. The first, called the Safe Harbor, was adopted in 2000, but was challenged at the EU Court of Justice (CJEU) by privacy activist Max Schrems in 2014, on the grounds that surveillance programs in the U.S. were overly-broad and did not conform to EU privacy law, a discovery catalyzed by Edward Snowden's disclosures regarding U.S. surveillance practices. Ultimately, the CJEU invalidated the Safe Harbor in October 2015, in C-362/14 ("**Schrems I**"). In 2016, the EU and U.S. reached another agreement, and the EC adopted the second adequacy decision, called the Privacy Shield. Schrems challenged this decision at the CJEU, on the grounds that the U.S. did not make any substantive improvements or enhancements to its surveillance or data privacy infrastructure. In July 2020, the CJEU invalidated the Privacy Shield in C-311/18 ("**Schrems II**"). In response to the adoption of the DPF, **Schrems has indicated** that he will challenge the third adequacy decision on the grounds that the framework is essentially a copy of the failed Privacy Shield. This process will likely take one or two years, reaching the CJEU in 2024 or 2025.

In the meantime, organizations that become certified will be able to immediately rely on the DPF in facilitating cross-border transfers of personal data. Further, organizations that participated in the Privacy Shield may immediately consider themselves certified and rely on the DPF, but will have to self-certify under the DPF by October 10, 2023.

While we are excited by the adoption of the DPF, we recognize that the framework may not be here to stay. In the event that it suffers the same fate as its predecessors, we are advising clients to exercise caution when making changes to their data privacy and security practices – a complete overhaul of the systems currently in place may have to be walked back in a year or two. Even so, we encourage our clients to take advantage of the streamlined DPF process.

© Copyright Babst, Calland, Clements and Zomnir, P.C.

National Law Review, Volume XIII, Number 203

Source URL:https://natlawreview.com/article/new-privacy-shield-european-commission-adopts-eu-us-data-privacy-framework