wiley

ALERT

Executive Order on EU-U.S. Data Sharing Signed

October 10, 2022

On October 7, 2022, President Biden signed the Enhancing Safeguards for United States Signals Intelligence Activities Executive Order (Executive Order or EO), which implements the EU-U.S. Data Privacy Framework (EU-U.S. DPF). Implementation of the EU-U.S. DPF is a crucial step in building a reliable and trusted data flow mechanism between the EU and U.S. to replace the invalidated EU-U.S. Privacy Shield Framework (Privacy Shield). Below we provide background on the cross-border data transfer issues that led to the creation of the EU-U.S. DPF, highlights of the EO, and an outline of next steps and timing for impacted businesses.

The Privacy Shield

The Privacy Shield was invalidated in July 2020 by the Court of Justice for the European Union (CJEU) in the *Schrems II* decision. In deciding *Schrems II*, the CJEU held that the Privacy Shield was not a valid data transfer mechanism under the General Data Protection Regulation (GDPR) because it did not provide an "adequate level" of privacy protection. Specifically, the Court determined that the Privacy Shield was insufficient to protect against U.S. national security surveillance – which the Court determined was not limited to what was "strictly necessary and proportional" as required by EU law – and did not provide individuals located in the EU with actionable judicial redress to protect their personal data. The invalidation of the Privacy Shield left thousands of U.S. businesses that had relied upon Privacy Shield without a clear means of transferring personal data from the EU to the U.S.

Authors

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Jacqueline F. "Lyn" Brown
Of Counsel
202.719.4114
jfbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

GDPR and Global Privacy

Privacy, Cyber & Data Governance

In the same decision, the CJEU affirmed the validity of transferring data via standard contractual clauses (SCCs). Subsequently, further guidance was provided by the European Data Protection Board (EDPB) on supplemental transfer tools and procedures that may be necessary to ensure data transfers between the EU and the U.S. provide the required level of safeguards for EU residents. In the two years since the *Schrems II* decision, many businesses that previously relied upon Privacy Shield implemented SCCs (and any additional transfer obligations required by the EDPB guidance) to bring their cross-border data transfers into compliance. However, businesses will welcome the EU-U.S. DPF as a more streamlined option for compliant EU to U.S. data transfers.

The Executive Order

The Executive Order is an essential first step in building out the successor to the Privacy Shield. In direct response to the *Schrems II* decision, the EO requires U.S. intelligence agencies to limit signals intelligence activities to those which are proportionate and necessary. Further, these activities shall be subject to "rigorous oversight." The EO will create a new multi-layer mechanism for oversight and redress review. Potentially impacted individuals, including EU individuals, will now be able to lodge a complaint about U.S. signals intelligence activity with the Civil Liberties Protection Officer (CLPO) in the Office of the Director of National Intelligence who will conduct an investigation and issue a binding independent decision. The CLPO's decision can then be independently reviewed by a new Data Protection Review Court created by regulations issued by the U.S. Department of Justice. This two-layer redress review mechanism represents a significant improvement from the previous Privacy Shield Ombudsman.

Next Steps

Next, the process moves to the European Commission (EC). The EC is responsible for preparing the draft adequacy decision and beginning the adoption process. The adoption process has several layers, including an approval process by a select committee of representatives of EU Member States and a right of scrutiny by the European Parliament. This process is expected to take between four and five months. And, for perspective, the Privacy Shield approval process took five months.

The U.S. Department of Commerce (U.S. DOC), in a press release issued shortly after the EO, noted that "[t]he EU-U.S. DPF will also update the privacy principles that companies adhere to under the EU-U.S. Privacy Shield Framework and rename them as the 'EU-U.S. Data Privacy Framework Principles.'" Companies that have continued to adhere to the Privacy Shield Principles during the past two years will be contacted by the U.S. DOC with next steps once the adequacy decision is finalized.

While the U.S. and EU authorities remain optimistic that the EU-U.S. DPF will ultimately result in an adequacy decision, it is highly likely that the decision will be subjected to legal challenges. Indeed, shortly after the EU and U.S. announced they had reached an agreement in principle in March 2022, Max Schrems stated "[w]e expect this to be back at the Court within months from a final decision."

In the expectation of further legal challenges, we encourage companies to continue to rely upon alternative compliant data transfer mechanisms (and any additional transfer obligations required by the EDPB guidance). And for businesses that have implemented SCCs – a reminder that you have until December 27, 2022 to amend existing contracts to incorporate the updated SCCs that were released in June 2021.

This Executive Order adds yet another landmark to the extremely active privacy landscape in the United States. On the horizon are five state omnibus privacy laws taking effect in 2023, the Federal Trade Commission's rulemaking on "Commercial Surveillance and Data Security," as well as potential federal bipartisan privacy legislation. We encourage businesses to remain vigilant to ensure that cross-border data transfers remain compliant with current obligations and hopeful that these transfers may soon become easier.

***

Wiley's Privacy, Cyber & Data Governance Team has helped companies of all sizes from various sectors proactively address risks and address compliance with new privacy laws and requirements. Please reach out to any of the authors with questions.