U.S. takes action to ease EU concerns over personal data transfers

Christine N. Czuprynski | Thursday, November 17, 2022

On October 7, 2022, President Joe Biden signed the Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities. The executive order sets forth the steps that the United States will take to implement the U.S. commitments under the European Union-U.S. Data Privacy Framework (EU-U.S. DPF) announced by President Biden and European Commission President Ursula von der Leyen on March 25, 2022.

Under the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), a transfer of personal data to a third country like the United States may take place where the Commission has decided that the third country in question ensures an adequate level of protection. *GDPR Article 45*.

The adequacy decisions for transferring personal data from the EU into the U.S. have endured a tumultuous history. On October 6, 2015, the European Court of Justice invalidated the U.S.-EU Safe Harbor Framework, which had been in place as a legal mechanism for onward transfer since July 2000. On July 12, 2016, the European Commission issued an adequacy decision on the EU-U.S. Privacy Shield Framework. The Privacy Shield replaced the Safe Harbor framework, but was immediately challenged as inadequate. On July 16, 2020, the Court of Justice of the European Union issued a judgment declaring as "invalid." The European Commission's Decision (EU) 2016/1250 on the adequacy of the protection was provided by the

EU-U.S. Privacy Shield. *See Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (*Schrems II*). As a result of that decision, the EU-U.S. Privacy Shield Framework was no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the U.S.

The reasons the European Court of Justice provided for invalidating the Privacy Shield Framework was summarized by Caitlin Fennessey at IAPP:

> First, the court found that U.S. surveillance programs, which the commission assessed in its Privacy Shield decision, are not limited to what is strictly necessary and proportional as required by EU law and hence do not meet the requirements of Article 52 of the EU Charter on Fundamental Rights. Second, the court determined that, with regard to U.S. surveillance, EU data subjects lack actionable judicial redress and, therefore, do not have a right to an effective remedy in the U.S., as required by Article 47 of the EU Charter.

The Trans-Atlantic Data Privacy Framework and executive order are meant to address those concerns. As the fact sheet from President Biden states:

> The new Trans-Atlantic Data Privacy Framework underscores our shared commitment to privacy, data protection, the rule of law, and our collective security as well as our mutual recognition of the importance of trans-Atlantic data flows to our respective citizens, economies, and societies. Data flows are critical to the trans-Atlantic economic relationship and for all companies large and small across all sectors of the economy. In fact, more data flows between the United States and Europe than anywhere else in the world, enabling the $7.1 trillion U.S.-EU economic relationship.

The president's Executive Order forms the basis of a draft adequacy decision by the European Commission to fully codify the new Trans-Atlantic Data Privacy Framework. Such an adequacy decision takes several months, so it could be March or April 2023 before we have that official word. And, following any such adequacy decision, we fully expect legal challenges and scrutiny as to whether the Executive Order satisfies all of the concerns raised in *Schrems II*.

In the meantime, companies should follow guidance from the European Data Protection Board (EDPB), provided in the wake of *Schrems II*. That guidance includes:

1. Know your transfers. Map and understand the transfers of personal data from the European Union to other countries/jurisdictions.
2. Verify your transfer mechanism. Match all transfers of personal data from the EU into other jurisdictions with the transfer mechanism on which you are relying.
3. Assess the legitimacy and effectiveness of the transfer mechanism. Determine if the relied-upon mechanism is not sufficient or adequate under current legal frameworks and guidance.
4. Identify and adopt supplementary measures. As needed, cure any insufficient transfer mechanisms.
5. Formalize the changes. As needed, formally adopt the supplementary measures and take other steps as required under the GDPR.
6. Re-evaluate at regular intervals. We have all witnessed the changes to this area. The data privacy principle of accountability requires constant assessment of the current status of the law and guidance.

We will bring further updates on the subject of transfers of personal data as they are available.

Christine N. Czuprynski