STINSON

News & Insights

EU Suspends the Privacy Shield – Where do we go from here?

Alert

07.17.2020

By David Jennings, CIPP/E and Steven Cosentino, CIPP

In a decision issued on July 16, 2020, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield Framework, one of the primary tools used by companies in the European Union (EU) to transfer personal data (as defined by the EU's General Data Protection Regulation or GDPR) to the U.S. The CJEU ruled that the Privacy Shield Framework is inadequate and fundamentally incompatible with the personal data protections intended to be afforded by the GDPR.

This case (commonly referred to as *Schrems II*) is the latest round of litigation between Facebook and Max Schrems, an Austrian privacy advocate. The *Schrems II* decision addresses two primary mechanisms used by companies large and small to export personal data from the EU as part of their ongoing business operations: (1) the EU-U.S. Privacy Shield Framework; and (2) use of written agreements that include non-negotiable, contract clauses pre-approved by the European Commission (known as standard contractual clauses or model clauses).

Invalidation of the Privacy Shield

After the CJEU invalidated the Safe Harbor, a predecessor to the Privacy Shield, in the first *Schrems* decision, many companies were skeptical about adopting the Privacy Shield. We now know that this skepticism was not without merit. The U.S. Department of Commerce and the European Commission implemented the Privacy Shield Framework to provide companies on both sides of the Atlantic with a better mechanism to comply with GDPR requirements when transferring personal data from the EU to the U.S. Evidentially, the new mechanism was not good enough, with the CJEU finding that it was not sufficient to guarantee a level of protection equivalent to that provided in the EU.

EU Suspends the Privacy Shield – Where do we go from here?

A third negotiated personal data transfer scheme to replace the Privacy Shield Framework seems unlikely. It took the European Commission, the EU executive, and the United States more than a year of negotiations to agree to the terms of the now defunct Privacy Shield Framework following the decision in *Schrems I*, which invalidated the prior Safe Harbor mechanism. While there may be hope that a new framework can be put in place, the *Schrems II* decision creates significant doubt that such a framework is even possible without some fundamental change to the reach of U.S. government surveillance mechanisms.

Since its inception, approximately 5,400 companies signed on to the Privacy Shield Framework through the self-certification mechanism established and operated by the U.S. Department of Commerce. The Privacy Shield Framework was designed to protect the personal data of European data subjects that is transferred outside the EU. This often includes transfers to processors in the U.S. engaging in a broad range of activities such as outsourcing, payroll and cloud services.

Scrutiny of Standard Contractual Clauses

Personal data transfers from the EU to the U.S. that rely on the standard contractual clauses for compliance with the GDPR remain, at present, a viable approach. Although the CJEU validated this second primary mechanism used to export personal data from the EU, the CJEU's decision creates significant uncertainty that the standard contract clause mechanism will continue to survive scrutiny from EU Data Protection Authorities in the future. This uncertainty is particularly concerning for countries with sophisticated government data collection capabilities such as the U.S.

More specifically, the CJEU ruled individual data protection authorities of EU member states, such as Ireland's DPC in the *Schrems* case, are required to suspend or prohibit a personal data transfer to a third country (including the U.S.) if, in the view of the authority and in light of all circumstances of the transfer, those clauses are not or cannot be complied with in the third country, and if the data controller or a data processor has not already suspended or ended the transfer. In short, if the Data Protection Authority of an EU member state determines that the same U.S. government national security laws (e.g., surveillance laws) that were the underlying cause of the invalidation of the Privacy Shield Framework do not adequately protect personal data in light of the requirements of the GDPR, then that Data Protection Authority must suspend or prohibit that particular transfer of personal data to the U.S. that is taking place pursuant to the standard data protection clauses. The language used by the CJEU indicates that such a determination should be made on a case-by-case basis, and such analyses may certainly involve nuanced application the GDPR's requirements.

Steps Companies Need to Take

EU Suspends the Privacy Shield – Where do we go from here?

If your company relies on the Privacy Shield Framework for personal data transfer from the EU, then you need to take immediate steps to adopt a replacement mechanism such as the standard contractual clauses. If you are a processor in the U.S., providing services to a controller in the EU, you should have a form of Data Protection Agreement ready to provide your EU customers that includes the clauses. Keep in mind that the transfer mechanism issue can apply at the subprocessor level. So if you are a processer with a flow down data protection agreement in place with a subprocessor who was relying on the Privacy Shield, that agreement must be revised to include standard contractual clauses as well. Finally, keep an eye out for new developments such as the invalidation of the use of standard contractual clauses in particular circumstances. We will be covering such new developments in subsequent alerts and guidance.

CONTACTS

Stephen J. Cosentino, CIPP

David B. Jennings, CIPP/E

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Intellectual Property & Technology