WINSTON & STRAWN LLP

BLOG

EU Court Strikes Down Privacy Shield and Causes Data Transfer Headaches for U.S. Companies

JULY 17, 2020

In a highly anticipated decision, the European Court of Justice (ECJ) announced a decision in the "Schrems II" case. The court considered legal transfer methods for the transfer of personal data to processors established in other countries and struck down the Privacy Shield as inadequate and failing to meet the protections required by the General Data Protection Regulation (GDPR), in effect since 2018, and used by over 5,300 U.S.-based companies. Activities enabled by Privacy Shield include Gmail or Zoom. The ECJ upheld Standard Contractual Clauses (SCC) as an available transfer mechanism accessible to companies.

The Schrems II case and its progeny (Schrems I) demonstrate the tension that exists between EU and U.S. privacy laws. These cases analyzed what protections were offered to personal data transferred from the EU to the U.S., and evaluated whether various programs between the U.S. and EU provided the level of protection required by the EU. Under the GDPR, there must be a legitimate basis to transfer data out of the country, and the transfer of such data to a third country "may . . . take place only if the third country . . . ensures an adequate level of data protection."[1] In its 2015 Schrems I ruling, the ECJ considered whether the Safe Harbour program complied with EU data protection requirements, and it deemed the Safe Harbour data transfer inadequate. In an attempt to remedy this shortcoming, the Privacy Shield program was adopted by agreement between the United States Commerce Department and the EU. The Privacy Shield program offered a means by which companies within the U.S. could "self-certify" their data transfers as adequate by complying with the data protection terms outlined in the Privacy Shield. Experts questioned whether the Privacy Shield mechanism would survive scrutiny of the ECJ given U.S. surveillance practices.

In Schrems II, the ECJ held that given the U.S.'s continued use of mass surveillance programs and the lack of adequate redress for Europeans, Privacy Shield fails to offer adequate protection, and more specifically the data of European citizens. "The limitations on the protection of personal data arising from the domestic law of the United States on the access and use by U.S. public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent," said the judgment. The ECJ found that "the requirements of U.S. national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country." What this means is that there is no guarantee that EU law's finely tuned privacy protections would be upheld in the U.S., once the data is transferred there. This ruling striking down the Privacy Shield program is not subject to appeal.

While the ECJ's ruling effectively nullified the Privacy Shield program as valid mechanism for the transfer for personal data from the European Union, the ECJ did uphold Standard Contractual Clauses as a mechanism to move data overseas. Standard Contractual Clauses (SCC) are contractual terms in which the sender and recipient of personal data agree on sufficient safeguards to protect the data. "The European Commission can decide that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally."[2]

The EU has issued two sets of model standard contractual clauses for data transfers to data controllers outside the EU, and one set of standard contractual clauses for data transfers to data processors outside the EU, to assist companies, and which are available here. It is unclear whether companies are now limited to using only the SCCs pre-approved by the Commission, or whether there will be a new alternative mechanism through which companies can have their data-transfer protocols deemed adequate. While individual Data Protection Authorities (DPAs) can always reject SCCs if it finds the proposed contract is not in conformity with the SCCs, companies should find some comfort by the fact that the SCCs have been used in their pre-approved form since 2001.

The other data transfer mechanism is through the use of Binding Corporate Rules, in which a company creates data protection policies for transfers of personal data outside the EU within a group of companies. Companies must submit corporate rules for approval to the competent data protection authority in the EU. This method is not favored as it requires time and expense working through the approvals of potentially several DPAs. The approval times vary in each of the EU jurisdictions.

This ruling will affect every company who transfers personal data from the EU to the U.S. The EU has sent a strong message that the data protection rights afforded to EU individuals must be respected in the U.S. This signals a growing divide between the European and U.S. approaches to data protection and may not be resolved absent major changes in the U.S. surveillance laws or the enactment of a Federal data protection law that ensures adequate data protection to the GDPR standards. Furthermore, the decision may signal problems for Brexit Britain, especially in light of the fact that the UK is trying to secure an EU data adequacy decision that will allow free movement of data between the EU to the UK after Brexit.

TIP: Companies should continue to monitor EU guidance as to standard contractual clauses requirements. Prior to transferring EU personal data to the U.S., companies should conduct the appropriate assessment of data protection adequacy and maintain records supporting their analysis. If your company has used Privacy Shield, a quick conversation with your legal counsel may be appropriate to determine best ways to safely transfer data across the Atlantic.

---

[1] https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[2] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

4 Min Read

Authors

John Rosenthal

Sara Susnjar

Virgile Puyau

Related Locations

Houston | Paris | Washington, DC

Related Topics

Europe Privacy

Data Breach

Related Capabilities

Privacy & Data Security

Privacy: Regulated Personal Information (RPI)

Related Regions

North America

Europe

Related Professionals

John Rosenthal

Sara Susnjar

Virgile Puyau

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.