VORYS

Publications

Privacy Alert: EU-U.S. Privacy Shield Invalidated by Europe's Court of Justice

Related Attorneys

Marcel C. Duhamel

Gretchen Rutz Leist

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 7.16.2020

On July 16, 2020, the Court of Justice of the European Union invalidated reliance on the EU-U.S. Privacy Shield program for the transfer of data from within the EU to entities within the U.S. The EU-U.S. Privacy Shield Framework, designed by the U.S. Department of Commerce and the European Commission, provided thousands of companies a mechanism by which to comply with the nations' different data protection requirements when transferring personal data to and from the EU and the U.S. Now, companies relying on the Privacy Shield will be forced to rapidly implement different privacy practices in order to legally transfer data across the Atlantic.

Summary of Ruling

On June 25, 2013, Austrian national Maximillian Schrems filed a complaint with the Irish Data Protection Commissioner against Facebook Ireland, Ltd., where he requested that Facebook Ireland, a subsidiary of Facebook Inc., be prohibited from transferring his personal data to the U.S. on the grounds that U.S. privacy law did not adequately protect his personal data. This complaint, though initially dismissed by the Irish regulator, eventually led to the European Court of Justice striking down the transatlantic U.S.-EU Safe Harbor agreement that enabled companies to transfer data from Europe to the United States.

The EU-U.S. Privacy Shield, created in 2016, was meant to replace the Safe Harbor agreement, providing stronger protections for the personal data of EU citizens when exported to the U.S. When Facebook certified to the EU-U.S. Privacy Shield Framework with the U.S. Department of Commerce, Schrems challenged the new data transfer mechanism. The new complaint found its way back to the European Court of Justice who once again ruled in favor of Schrems.

In its decision invalidating the EU-U.S. Privacy Shield, the Court of Justice expressed concerns that the Privacy Shield did not adequately protect the data of EU citizens from U.S. surveillance activities. Specifically, the Court found that U.S. national law does not ensure the

level of protection required by the GDPR—the EU's General Data Protection Regulation—because, in the United States, the interests of national security, public interest, and law enforcement have primacy over the fundamental privacy rights "guaranteed within the European Union" by virtue of the GDPR.

The Court was most concerned about the adequacy of U.S. protections against government surveillance programs (such as FISA), finding that data subjects have "no right to an effective remedy" with respect to those surveillance programs. The Court took special note of the difficulty a resident of the EU would have in establishing the standing necessary to sue a US intelligence service in a US court for violation of privacy rights guaranteed by GDPR. While the Privacy Shield program provides for a Privacy Shield Ombudsman, the Court found that the Ombudsman could not provide a meaningful and effective judicial remedy in the event of a US intelligence service's interception or surveillance of personal data. Because the U.S. does not offer protections against government surveillance equivalent to those provided by the GDPR, the Court held that the Privacy Shield program is incompatible with the GDPR.

Alternative Options for Data Transfers from the EU to the U.S.

Other options do exist for the transfer of data to the United States.

Privacy Shield is only one mechanism provided by GDPR to effectuate transfers out of the EU to countries, like the United States, not deemed to provide adequate protection, although the extent to which these mechanisms may be available for transfers to the US may be in some doubt. For example, GDPR generally permits such transfers where the transferor and the transferee have entered "standard contractual clauses" that have been approved by the relevant data supervisory authority and the European Commission, although the *Schrems 2* decision may suggest that, in the case of transfers to the U.S., these clauses may be inadequate to the extent they are not enforceable against U.S. intelligence services. Another mechanism is adoption of "binding corporate rules," which might permit transfers between two related corporate entities, but here too these binding corporate rules must be approved by a supervisory authority and again the question remains whether they can be enforced against the U.S. government if it intercepts or surveilles data transfers.

GDPR itself also provides "derogations," or exceptions, to the general prohibition on data transfers to entities located in jurisdictions not deemed to provide adequate protection. For example, transfers are generally permissible where the data subject consents after having been informed of the possible risks due to the absence of an adequacy decision by the European Commission and due to the absence of appropriate safeguards in the United States. Other exceptions include:

- Where the transfer is necessary to perform a contract between the data subject and the controller, or to take pre-contractual steps at the data subject's request
- Where the transfer is necessary to perform or make a contract between the controller and a third party, if the contract is made "in the interest of the data subject"
- Where the transfer is necessary for "important reasons of public interest"
- Where the transfer is necessary for the establishment, exercise or defense of legal claims
- Where the transfer is necessary for the "vital interests" of the data subject or other persons and the data subject is physically or legally incapable of consent

- Where the transfer is from a public register satisfying specific requirements

Conclusion

U.S.-based entities that have relied on Privacy Shield certification to receive personal data from entities located within the EU—including corporate affiliates transferring data from the EU to the U.S. affiliate—must now reassess whether those data transfers remain lawful under GDPR. Whether alternative mechanisms such as reliance on standard contractual clauses will be available may be an open issue. Those companies wishing to rely on the "derogations" instead will be well-advised to consider carefully, on a case-by-case basis, whether those derogations are applicable to the specific data being transferred.