Time To Reassess International Data Transfers After Court Declares EU-U.S. Privacy Shield Invalid: A 4-Step Action Plan

Insights
7.22.20

The Court of Justice of the European Union just ruled that an important data protection scheme established between the European Union and the United States is invalid, calling into question many aspects of important data transfers carried out by private businesses in America. In what is being referred to as the "*Schrems II*" decision, the July 16 decision invalidating the EU-U.S. Privacy Shield reinforces the importance of data protection. It raises important questions as to the future of international data flows and use of data transfer mechanisms between the EU and companies around the globe, but especially those in the U.S.

The immediate result: more than 5,300 companies who currently rely on the EU-U.S. Privacy Shield Framework for international data transfers must reassess their data transfer mechanisms. Below you will find a summary of the situation and a four-step action plan to address immediate concerns.

Background
For the past 25 years, European Union data protection laws – first the Data Protection Directive and then the General Data Protection Regulation (GDPR) – have restricted the free transfer of EU personal data outside the EU and European Economic Area (EEA), which includes all EU countries, Iceland, Liechtenstein, and Norway. This means the vast majority of transfers of EU personal data outside the EU/EEA, including those to the U.S., must be covered by a legal data transfer mechanism such as European Commission-approved Standard Contractual Clauses (SCCs) or the EU-U.S. Privacy Shield Framework.

- SCCs are standardized contractual clauses used in agreements between service providers and their customers to ensure that any personal data leaving the EEA will be transferred in compliance with EU privacy laws.
- The EU-U.S. Privacy Shield Framework is a 2016 agreement designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU to the U.S.

Schrems I
In 2013, Austrian Maximillian Schrems filed a claim against Facebook, complaining that the social media company had supposedly gathered over 1,200 pages of his personal information. He asked the Irish Data Protection Commissioner to prohibit personal data transfers to the U.S., claiming that U.S.

Irish Data Protection Commissioner to prohibit personal data transfers to the U.S., claiming that U.S. laws and practices did not adequately protect personal data from the surveillance activities of its public authorities.

The Irish DPC initially rejected Schrems' complaint, pointing to the "Safe Harbor" provision of the 1995 EU Privacy Directive 94/46/EC. That Directive stated that U.S. companies may collect an EU user's personal data after obtaining their consent if there is an "adequate level of data protection." But after Mr. Schrems appealed to the European Court of Justice (ECJ), the court ruled in 2015 that Safe Harbor provisions were incompatible with the right to privacy under the existing EU Directive.

Schrems II

Schrems continued his fight before the Court of Justice of the European Union (CJEU), seeking a determination that U.S. legislation does not ensure adequate protection of personal data of EU citizens. He also challenged whether the use of SCCs offered sufficient safeguards as to the protection of EU citizens' freedoms and fundamental rights.

Court Upholds SCCs – On Certain Conditions

In *Schrems II*, the CJEU reaffirmed the validity of SCCs as a valid transfer mechanism. However, it issued a caveat that companies must verify, on a case-by-case basis, whether the law in the recipient country offers a level of data protection that is essentially equivalent to that of the EU. Where protections in the recipient country are inadequate, companies must provide additional safeguards or suspend transfers. The court further held that EU Member State data protection authorities are required to suspend such transfers on a case-by-case basis where equivalent protection cannot be ensured.

This aspect of the *Schrems II* decision may have troubling implications for U.S. companies, as the CJEU assessed the sufficiency of protections with regard to U.S. government access to data and found them lacking. The question U.S. regulators and companies now face is whether the concerns raised by the CJEU are applicable in the context of particular transfers and can be remedied through additional protections.

Court Invalidates Privacy Shield

While the CJEU confirmed the use of SCCs, it held that the other data transfer mechanism – the EU-U.S. Privacy Shield – does not include satisfactory limitations to ensure the protection of EU personal data from access and use by U.S. public authorities on the basis of U.S. domestic law. The practical result is that the EU-U.S. Privacy Shield decision can no longer be relied upon for EU-U.S. data transfers.

The CJEU invalidated the framework based on its finding that U.S. surveillance law does not include the safeguards required to meet EU data protection principles concerning proportionality, meaning the collection of data is not limited to what is necessary. Further, the CJEU found that, with regard to U.S. surveillance, EU data subjects lack a meaningful remedy before a body that offers guarantees substantially equivalent to those under EU law. In particular, the CJEU reasoned that the Privacy

Shield's Ombudsperson is not sufficiently independent and is unable to adopt decisions that bind U.S. intelligence services.

How Has the U.S. Responded?

Shortly after the CJEU issued the *Shrems II* decision, the U.S. Department of Commerce (which administers the Privacy Shield framework in the U.S.) quickly issued a statement that Secretary Wilbur Ross is "deeply disappointed" in the invalidation of the EU-U.S. Privacy Shield. However, he also said that the department has "been and will remain in close contact with the European Commission and European Data Protection Board on this matter and hope to be able to limit the negative consequences to the $7.1 trillion (trans-Atlantic) economic relationship that is so vital to our respective citizens, companies, and governments." European Commission authorities echoed this sentiment in collaboration during a news conference held shortly after the ruling.

What Companies Should Do Now: A 4-Step Action Plan

Organizations who engage in any kind of personal data transfers outside of the EU/EEA must carefully evaluate the ramifications of the *Schrems II* ruling and consider taking the following steps:

1. **Switch from Privacy Shield to alternative safeguards:**Companies that have until now relied upon the EU-U.S. Privacy Shield will need to look for an alternative legal basis to enable transfers under the GDPR. Current participants in the Privacy Shield will need to bear in mind that EU personal data previously transferred to the U.S. under the Privacy Shield framework must be returned or remain subject to safeguards implemented in accordance with the Privacy Shield principles. Entities that choose to withdraw from the Privacy Shield framework must still continue to apply the Privacy Shield principles to any EU data received while they participated in the Privacy Shield.
2. **Verify level of protection of international data flows:** Although companies can continue to use the EU SCCs as a safeguard for transferring personal data to processors outside the EU/EEA, you will have to follow the level of data protection provided in the third country and, where conflicts with the provisions of the SCCs arise, to suspend data exports.
3. **Monitor activities on updated SCCs:** The EU Commission confirmed it is working on alternative instruments for international transfers of personal data, including by reviewing the existing SCCs. You should closely follow further developments of new safeguards as announced by the EU Commission.
4. **Assess strategies for compliance with U.S. and EU laws:** In the context of litigation, organizations subject to both U.S. law and the GDPR should assess whether they have a strategy in place for responding to discovery requests that may implicate the disclosure of EU personal data, as U.S. legal obligations may be at odds with EU data protection requirements.

Fisher Phillips will continue to monitor this situation and provide updates as appropriate. Make sure you are subscribed to Fisher Phillips' Alert System to get the most up-to-date information. For

additional information about compliance, contact your Fisher Phillips attorney or any attorney in our Privacy and Cyber Practice Group.

This Legal Alert provides an overview of a specific international law development. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Service Focus

Privacy and Cyber

International

Consumer Privacy Team