Updates
July 20, 2020
EU Court Strikes Down EU-US Privacy Shield

The Court of Justice for the European Union (CJEU) on July 16, 2020, invalidated the EU-U.S. Privacy Shield as an approved mechanism for transferring personal data from the European Union to the United States. This decision will significantly affect how thousands of companies process the personal data of EU data subjects and engage in international trade.

The CJEU's decision rests largely on its determination that the Privacy Shield program cannot protect personal data that is exported to the United States from government access pursuant to U.S. national security laws. Companies that previously relied on the Privacy Shield framework to facilitate EU-U.S. data transfers now need to find another lawful mechanism for carrying out these transfers or suspend the transfers and process the data only in the EU. For many companies, that will entail putting into place Standard Contractual Clauses (although the CJEU judgment also calls into question whether SCCs provide sufficient safeguards with respect to transfers from the EU to the United States).

Background

European data protection law restricts the flow of personal data from the EU to countries, including the United States, that are deemed to have an "inadequate" data protection regime in place. Data transfers from the EU to the United States are permitted only if an approved mechanism is in place, such as the EU SCCs, Binding Corporate Rules (BCRs), or an international agreement such as the Privacy Shield framework. Transferring data outside of the EU in violation of these restrictions may be considered a serious infringement of the GDPR, subject to a fine of up to the greater of €20 million or 4% of the firm's worldwide annual revenue from the preceding financial year.

The Privacy Shield was adopted by the U.S. Department of Commerce and the European Commission in 2016. By completing an online self-certification, participating companies committed to adhere to seven privacy principles when processing EU data subject personal data, including notice, choice, and accountability for onward transfer. For companies participating in the Privacy Shield program, the commission deemed the United States adequate and transfers from the EU to the United States were therefore allowed without another transfer mechanism (such as SCCs or BCRs).

The July 16 decision, *Data Protection Commission v. Facebook Ireland Ltd, Maximillian Schrems* (*Schrems II*), echoes themes from a prior case, *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*), which invalidated the Privacy Shield's predecessor, the Safe Harbor program.

In *Schrems I*, the CJEU held that the Safe Harbor program did not provide an adequate level of protection for the privacy and data protection rights of EU data subjects, largely because the Safe Harbor program broadly permitted processing for purposes of responding to U.S. national security and law enforcement requests. After the CJEU invalidated the Safe Harbor program, the United States amended several of its surveillance laws and, on that basis, the U.S. Department of Commerce and the European Commission created the Privacy Shield framework. Schrems immediately challenged the Privacy Shield framework, raising ongoing concerns regarding U.S. national security practices. After consideration by the Irish Office of Data Protection Commissioner and Irish national courts, several questions of EU law were referred to the CJEU, resulting in the *Schrems II* judgment.

CJEU Decision

The CJEU concluded in *Schrems II* that the EU-U.S. Privacy Shield does not provide an adequate level of protection and, as a result, is not a valid mechanism for lawful transfers of personal data from the EU to the United States under the EU's General Data Protection Regulation (GDPR). Specifically, the CJEU doubted whether U.S. law provides the level of protection required by EU law in light of specific national security authorities pursuant to which the U.S. government may seek access to personal data.

The Privacy Shield agreement states that adherence to the Privacy Shield Principles may be limited "to the extent necessary to meet national security, public interest, or law enforcement requirements." The CJEU found this language to be similar to language in the Safe Harbor program that appeared to create an exception to the program's privacy protections allowing the U.S. government relatively unrestricted access to EU data subject personal data for national security purposes.

The CJEU also found with respect to U.S. government access to personal data that EU data subjects had no effective means of redress. Although the Privacy Shield permits EU data subjects to request information regarding the U.S. government's processing of their personal data to an ombudsperson, the CJEU found that the ombudsperson did not provide an independent, effective means of seeking redress as required by EU law. The CJEU noted that the ombudsperson mechanism within the Privacy Shield is not independent from the executive branch, particularly since there is a lack of protection against dismissal of appointment by the secretary of state, and that an ombudsperson's decisions are not binding on U.S. intelligence services. (Strangely, the CJEU judgment did not mention the Judicial Redress Act of 2015, enacted to extend to foreign citizens certain rights of judicial redress established for U.S. citizens under the Privacy Act of 1974.)

The CJEU confirmed that SCCs remain a valid mechanism under the GDPR for transferring data, but it did introduce a degree of uncertainty as to their continued viability for the very reasons it invalidated the Privacy Shield. In particular, the court pointed to the obligation of the non-EU data importer to notify the data exporter if it was subject to local laws threatening its ability to comply with the obligations set forth in the SCCs. Whether SCCs remain a viable mechanism for transfer of data from the EU to the United States bears careful monitoring as companies work with data protection authorities to bring their practices into conformity with the CJEU's judgment.

Early Reactions From EU Authorities

Several EU authorities have weighed in with preliminary thoughts on the impact of the CJEU decision:

- EU data protection authorities have expressed some skepticism that the transfer of data from the EU to the United States pursuant to *any* mechanism, including the SCCs and BCRs, can comply with the GDPR in light of U.S. surveillance laws.
- Some data importers may be able to incorporate additional safeguards into their SCCs by representing that they have not and are not likely to receive requests from the U.S. government under the two national security authorities in question, Section 702 or Executive Order 12333.
- Data importers also may be able to implement additional security measures, such as end-to-end encryption, to further protect transferred data from surveillance.
- Companies relying on SCCs must assess whether the safeguards they are able to implement are adequate in light of the legal environment. If a data importer concludes that the safeguards do not result in adequate protection of EU data subject data, it must so inform the data exporter.

- GDPR data transfer derogations remain an option for certain data transfers, but authorities caution that derogations are meant for limited use, under very specific circumstances, and are generally unlikely to be appropriate for large-scale or continuous data transfer scenarios.

Next Steps?

If history is any precedent, we expect that the EU will provide guidance on how companies affected by this decision should approach EU-U.S. data transfers going forward. After the CJEU struck down the Safe Harbor framework, the EU provided an enforcement grace period for participating companies, both to provide time for the United States and EU to negotiate a new agreement and for companies to operationalize an approved alternative. We are hopeful they will do the same in this case.

In the meantime, we recommend that companies that were relying on the Privacy Shield adopt an alternative method for lawfully transferring data. For example, consider amending any data processing addenda (DPAs) which companies have signed with vendors or customers to incorporate the EU Standard Contract Clauses. Keep in mind, however, that the CJEU has recommended that companies include "additional safeguards" above and beyond the text of the Standard Contract Clauses. A company may be able to represent that it is not the kind of company subject to section 702 and/or that it has never received a request for data under section 702 or Executive Order 12333. Companies may also be able to commit to additional data security controls to better protect data from government surveillance. We recommend consulting with counsel regarding the additional safeguards that may be available.

Companies may also want to consider whether any of the derogations under GDPR Article 49 may apply. Article 49 permits, under some circumstances, transfers of personal data based on contractual necessity, data subject consent, and transfers upon the data subject's request, although each derogation is subject to its own operational limitations.

Where practical, companies may also want to consider whether EU-U.S. data transfers are essential to their business. If a company can store and process EU data subject data solely in the EU or another "adequate" jurisdiction, it might avoid these EU to United States data transfer requirements entirely. Note, however, that this approach may prevent a company's U.S. entities from accessing EU data subject data at all; even accessing the data from the United States may be considered a "transfer."

Finally, U.S. companies may want to engage with representatives of the U.S. government. They may want to encourage Congress to review U.S. surveillance laws or urge the executive branch to work urgently with the EU to negotiate a new data transfer framework. Companies may also want to watch for news regarding whether Switzerland and the United Kingdom follow the CJEU's lead and call into question the legality of transfers of personal data from their countries to the United States.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law