KPMG

Schrems II

What it means for US organizations & how they handle European personal data

What happened

On July 16, 2020, the Court of Justice of the European Union (CJEU) concluded in its *Schrems II* decision that the EU-U.S. Privacy Shield framework was no longer a valid mechanism for European organizations to rely on when transferring personal data to US companies for processing. The Court held that the Privacy Shield framework cannot guarantee EU citizens the fundamental right to privacy and data protection based on US surveillance laws.

Schrems II also added a burden on organizations that currently rely on Standard Contractual Clauses (SSC) to support data transfers from the EU by requiring personal data exporters to assess the impact of US national security laws on US data importers' ability to respect Europeans' privacy and data protection rights. The CJEU decision applies immediately and requires European data exporters and their recipients in the US to review and enhance their data protection practices relating to making personal data available to government national security and law enforcement agencies.

What are organizations doing and what should they consider

Many organizations are seeking legal opinions on the impact of this decision on their business practices. In order to best support the legal advisors on this impact, US organizations expecting to use SCC to govern importation of personal data from Europe should assess and gain visibility into their personal data transfer practices.

How KPMG can help

Perform a personal data transfer assessment (PDTA)

Step 1

Map export of European personal data to US

- Develop an inventory of European personal data transferred to the US
- Analyze each category of data transfer covered either by the Privacy Shield framework (recognizing that some industries are excluded), SSCs, or both
- Evaluate existing data protection controls against data protection provisions of the SSCs in place
- Assess whether personal data is encrypted to protect against electronic surveillance and potential interception during international transfer
- Determine whether data subjects have been informed of, and consented to, the potential exposure of their personal information to government security and law enforcement agencies
- Identify transfers of personal data to the US which may be necessary or otherwise permitted under GDPR Article 49, including among others performance of a contract or business transactions that logically need a transfer of personal data

Step 2

Perform privacy impact assessments (PIA)

- Work with legal advisors to determine if the US data importer may be considered an "electronic communication service provider" subject to US surveillance laws, or uses such providers to receive and/or transfer data between Europe and the US
- Compare the safeguards and remedies the data importer makes available to European data subjects to those of the data exporter and assess whether they are "essentially equivalent"
- Determine whether personal data is (or can be) anonymized prior to transfer
- Recommend privacy-enhancing practices for the organization's privacy by design program
- Socialize and detail findings of PIAs with the organization and its legal advisor

Step 3

Consider necessity of cloud relocation

- Should the organization and its counsel determine that revising SCCs or other methods are infeasible, develop an action plan for relocating personal data to a servers or hosting providers in the European Economic Area or in countries that have received adequacy findings from the European Commission
- Identify potential replacement providers, data residency considerations, and likely business disruption considerations

Conclusion

Schrems II has wide-ranging impact to organizations that process and/or control European personal data. Now is the ideal time to obtain greater visibility into your company's data and transfer practices—specifically processes that result in the transfer of European personal data to the US. With greater visibility, organizations can better protect data and enhance trust between customers, employees, and regulators.

At KPMG, our privacy team stands ready to assist your company in this important and time-sensitive effort. We encourage your organization to make the triad of visibility, protection, and trust the cornerstone of your privacy program.

Contact us

Steven Stein
Principal
KPMG Cyber Services
Privacy Services Co-Lead
T: 312-665-3181
E: ssstein@kpmg.com

Orson Lucas
Principal
KPMG Cyber Services
Privacy Services Co-Lead
T: 813-301-2025
E: olucas@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia