wiley

NEWSLETTER

European Authorities and FTC Provide Further Guidance on Privacy Shield

August 2020

Privacy in Focus®

European data authorities and the Federal Trade Commission (FTC) have provided additional guidance on how they will treat EU-U.S. data transfers after a landmark European court decision – suggesting that companies must adapt quickly to the shift or face enforcement actions. On July 16, 2020, the Court of Justice for the European Union (CJEU) upended the settled framework for companies to transfer personal data from Europe to the U.S., invalidating the EU-U.S. Privacy Shield Program (Privacy Shield) as a legal transfer mechanism and raising significant questions about the use of its primary alternative, Standard Contractual Clauses (SCCs). The Court's decision, known as *Schrems II*, has left U.S. companies scrambling to evaluate and implement alternative frameworks in order to legally transfer personal data from the EU.

The European Data Protection Board (EDPB) and a number of individual countries' Data Protection Agencies (DPAs) now have made clear that there is no automatic grace period for complying with the *Schrems II* ruling, meaning that companies relying on Privacy Shield or SCCs to authorize cross-border transfers must move swiftly to identify and implement alternate mechanisms, or stop the transfer of data out of the EU. At the same time, the FTC indicated at a hearing, on August 5, that it will continue to enforce any privacy representations that U.S. companies made as part of certifying compliance with the Privacy Shield framework – even after the *Schrems II* decision.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

GDPR and Global Privacy
International Trade
Privacy, Cyber & Data Governance
Telecom, Media & Technology

We outline five key takeaways for businesses below:

Businesses cannot count on a grace period for enforcement. Following the *Schrems II* decision, the EDPB released a FAQ affirming that the decision does not provide a grace period where companies can rely on Privacy Shield as a valid data transfer mechanism. In the weeks since the decision was released, individual DPAs continue to weigh in. Some DPAs – such as Ireland, Netherlands and Spain – are taking a measured approach affirming their commitment to cooperating with other European Authorities to adopt a common approach to enforcement, and a willingness to accept further guidance from the EDPB. Others, such as the German-Rhineland-Pfalz DPA state that any transfer made pursuant to Privacy Shield after July 16 is illegal and that data must be reclaimed or destroyed. And while the U.S. and European Commission officials, on July 10, 2020, announced discussions to consider a potential "enhanced" Privacy Framework, the process of developing a revised framework will take time.

Businesses using Standard Contractual Clauses for data transfer need to re-evaluate them in light of the national surveillance concerns in *Schrems II*. The EDPB's FAQ affirmed that a company that transfers data pursuant to SCCs or Binding Corporate Rules (BCRs) must conduct a secondary analysis to ensure the transfer is consistent with GDPR principles, as further outlined in the *Schrems II* decision. *Schrems II*, as we've noted, was primarily based on concerns that the U.S. government could obtain information about EU subjects under its national security laws specifically the Foreign Intelligence Surveillance Act (FISA). The concern in *Schrems II* was that U.S. law allows for a greater degree of surveillance of personal data, at least for electronic communications providers, than allowed under the GDPR. Companies that have been using SCCs or BCRs for data transfers may not necessarily have factored these concerns into their use of these mechanisms, and they now need to re-evaluate the risk that their data transfers may be deemed invalid. This analysis could include evaluation of what kinds of data about foreign individuals is subject to U.S. national security laws and how (or whether) data is encrypted or stored.

Use of cloud computing for storing EU personal data must be closely examined. As a related point, given the surveillance concerns discussed in *Schrems II*, the use of cloud services to process and store EU personal data outside of the EU will be under significant scrutiny by DPAs. Some of the largest cloud service providers are based in countries that have been assessed as having inadequate protections under the GDPR – including the U.S., China, and India. This hard line has some companies assessing whether they must use only EU-based cloud providers.

"Derogations" remain a valid option in some circumstances - but the scope is limited. The GDPR provides for certain situations when data transfers may be made even without an adequacy decision or other safeguards. The most commonly used derogations are with the explicit consent of the data subject, or when the transfer is necessary for the performance of a contract. However, the EDPB has cautioned that derogations are not meant to be used for "routine" or "ongoing" transfers. Thus, companies will want to carefully consider the use of derogations when evaluating both short-term and long-term data transfer options.

The FTC will continue to enforce Privacy Shield certifications. In the meantime, the FTC will continue to enforce U.S. companies' representations of Privacy Shield compliance, even though it is no longer a valid transfer mechanism. At a Congressional hearing on August 5, FTC Chairman Simons stated that companies that have certified compliance with the previous Privacy Shield framework still will be held to their promises about compliance. As a result, companies that are currently certified under Privacy Shield have continuing obligations as to data transferred under the framework, even if companies change practices going forward. The FTC retains the authority to enforce the FTC Act against companies that act inconsistently with their Privacy Shield representations.

Schrems II and the subsequent feedback from the EDPB and DPAs have disrupted EU-US data flows. While we anticipate additional guidance from the relevant authorities in the coming months, businesses must act now to assess the risk of data transfers between the EU-US and ensure use of a compliant transfer mechanism.

***

Wiley's Privacy, Cyber, and Data Governance Practice advises on GDPR compliance and domestic and international data transfer obligations. Please contact any of the authors for further information.