wiley

ALERT

Cross-Border Data Transfer Mechanisms in Flux as Court of Justice for the European Union Invalidates Privacy Shield

July 16, 2020

On July 16, 2020, the Court of Justice for the European Union (CJEU) issued a landmark decision invalidating the EU-U.S. Privacy Shield framework as an approved data transfer mechanism, leaving potentially thousands of U.S. companies without an approved mechanism to transfer information from the European Union (EU) to the United States.

The decision in *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (C-311/18) (*Schrems II*) considered the sufficiency of two commonly used data transfer mechanisms: Standard Contractual Clauses (SCCs) and the EU–U.S. Privacy Shield (Privacy Shield). The CJEU validated SCCs, with certain qualifications, but invalidated Privacy Shield. Companies that have been relying on the Privacy Shield framework for cross-border data transfers must now consider SCCs or other alternatives.

What does this mean for businesses that rely on Privacy Shield?

The *Schrems II* decision held that the Privacy Shield framework for EU-U.S. data transfers – negotiated by the United States and the European Commission and used by thousands of companies that certify compliance – was not valid under the General Data Protection Regulation (GDPR) because it did not provide an "adequate level" of privacy protection. The *Schrems II* decision itself provides no grace period for businesses to replace compliance with the Privacy Shield framework with another data transfer mechanism. As a result, effective today, businesses that have relied on Privacy Shield to transfer data from the EU to the United States must quickly identify an

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Of Counsel
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

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

alternative mechanism for the lawful transfer of data.

Although no explicit grace period was provided for in the decision, individual Data Protection Authorities (DPAs) still may take a measured approach to enforcement as they did when the precursor to Privacy Shield—Safe Harbor—was invalidated, potentially providing time for companies to find alternate means to legally transfer data.

Additionally, a business that has certified compliance with the Privacy Shield program is still subject to Privacy Shield obligations and enforcement in the United States. Although Privacy Shield is invalidated as a transfer mechanism by this decision, the business remains obligated – for enforcement purposes—to comply with the certifications made in its Privacy Shield registration. Indeed, in a press release issued shortly after the *Schrems II* decision, the U.S. Department of Commerce (DoC) affirmed that it will continue to administer the program and "[t]oday's decision does not relieve participating organizations of their Privacy Shield obligations." Thus, as businesses pivot to alternative data transfer mechanisms, they should also evaluate their obligations under the Privacy Shield program.

What are the options for businesses that have relied on Privacy Shield?

Separate from Privacy Shield, there are several other data transfer mechanisms that have been determined to provide appropriate safeguards under the GDPR. These include SCCs, which were validated by today's decision, Binding Corporate Rules (BCRs), and derogations as allowed by Article 49 of the GDPR.

Standard Contractual Clauses: The European Commission has approved three versions of SCCs: two that cover transfers from an EU controller to a non-EU controller, and one that covers a transfer from an EU controller to a non-EU processor. The *Schrems II* decision validated the use of SCCs, although when used by a U.S.-based company, the use of such clauses may be subject to a case-by-case review by an individual DPA to ensure the SCCs provide appropriate safeguards. Companies will need to closely analyze the SCCs they use and how they are implemented in light of today's decision.

Derogations: 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 European Data Protection Board (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.

Binding Corporate Rules: BCRs have long been the "gold-standard" of data transfer mechanisms. BCRs are created in direct consultation with a DPA. Typically, BCRs are used by large companies with wide-ranging data transfer obligations as they can take years to negotiate and involve great expense.

***

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.