

CLIENT ALERT

Privacy Shield Invalidated: EU Data Transfers to the U.S. under Siege (again...)

Jul.16.2020

At 9:30 a.m. Central European Time, privacy professionals around the world were refreshing their browsers to read the long-awaited judgment of the Court of Justice of the European Union (CJEU) principally addressing the viability of Standard Contractual Clauses (SCCs) and the EU-U.S. Privacy Shield (Privacy Shield) as means to transfer personal data from the European Union (EU) to the United States (U.S.).

When the judgment arrived, it landed with a bang: though the CJEU upheld the use of SCCs, it invalidated the Privacy Shield, the well-known mechanism to transfer personal data from the EU to the U.S. The decision also cast doubt on the viability of other options, including SCCs, for making transatlantic transfers.

The foundation of this decision and previous decisions affirming challenges to U.S. privacy practices is that the protection of personal data is a fundamental right in the EU, akin to a constitutional right in the U.S. The General Data Protection Regulation (GDPR) enshrined these fundamental rights and established uniform data protection standards across the EU designed to protect the personal data of EU-based individuals.

Protecting these fundamental rights when data is transferred abroad falls to the European Commission (EC). The EC can decide that certain countries provide an “adequate” level of protection for personal data thereby permitting the transfer of personal data to those countries.

In 2000, the EC put in place an adequacy mechanism known as the “Safe Harbour” for personal data transfers to the U.S. It was invalidated by the CJEU in 2015 ([Schrems I, case C-362/14](#)) due in large part to U.S. surveillance practices that arose in the wake of 9/11. It was replaced in 2016 by the Privacy Shield, which aimed to address the concerns that the CJEU outlined in its [Schrems I](#) judgment.

The CJEU has now also invalidated the Privacy Shield ([Schrems II, case C-311/18](#)) based on ongoing concerns regarding certain U.S. surveillance programs and their effect on the guaranteed privacy rights of EU-based individuals under the GDPR.

The CJEU came to this conclusion despite the fact that the U.S. “[...] participated actively in the case with the aim of providing the court with a full understanding of U.S. national security data access laws and practices and how such measures meet, and in most cases exceed, the rules governing such access in foreign jurisdictions, including in Europe,” as underlined in today’s [statement of U.S. Secretary of Commerce Wilbur Ross](#).

The Court also looked at [SCCs for processors](#), a mechanism that was created by the EC to facilitate international data transfer from the EU to non-EU vendors. While the CJEU did not invalidate this mechanism, it did underline that it is up to the exporting and importing organizations to verify that the legal system of the country where the recipient organization resides provides sufficient safeguards.

The Court's decision places EU transferring companies and recipient U.S. companies in a bind. U.S. companies can no longer rely on the Privacy Shield to receive data from the EU. While the CJEU upheld the legality of the SSCs, it now leaves it up to each EU exporting company to make its own decision regarding the integrity of U.S. privacy practices before deciding whether to transfer EU data to a U.S. company. And given that the CJEU has itself now invalidated the Privacy Shield based on its finding that the privacy practices of the U.S. government are deficient, an EU company contemplating entering into SCCs with a U.S. company will be faced with a difficult decision.

The Irish Data Protection Commission, the authority that passed this case to the CJEU, raises similar concerns in its statement: “[...] it is clear that, in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable.” It adds that the issue “will require further and careful examination, not least because assessments will need to be made on a case by case basis.”

Today's judgment is expected to significantly disrupt cross-Atlantic personal data transfers and the business models that rely on them in the short term. It remains to be seen what position European data protection authorities will take with regard to companies that rely on existing Privacy Shield certifications. A pragmatic approach with a *de facto* grace period (which, for the avoidance of doubt, is not foreseen in the CJEU's judgement), at least until there is a solid data transfer solution, seems to make the most sense.

Until these issues are resolved, affected businesses would likely benefit from ensuring that all data transfers and the corresponding data transfer mechanisms are duly mapped. Organizations relying on Privacy Shield certifications should also consider implementing other data transfer mechanisms such as SCCs while they remain an option or assessing whether derogations such as consent or contractual necessity can be relied upon.

Binding Corporate Rules that are approved by EU data protection authorities, may provide another solution to affected businesses recognizing that they can be used only for companies of the same corporate group or companies engaged in a joint economic activity.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Robert Holleyman

Partner and C&M International President & CEO – Washington, D.C.

Phone: +1 202.624.2505

Email: rholleyman@crowell.com

Jeffrey L. Poston

Partner – Washington, D.C.

Phone: +1 202.624.2775

Email: jposton@crowell.com

Maarten Stassen

Partner – Brussels

Phone: +32.2.214.2837

Email: mstassen@crowell.com

Jeane A. Thomas, CIPP/E

Partner – Washington, D.C., Brussels
Phone: +1 202.624.2877, +32.2.282.4082
Email: jthomas@crowell.com

Frederik Van Remoortel

Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com

Jarno Vanto, CIPP/E, CIPP/US

Partner – New York
Phone: +1 212.803.4025
Email: jvanto@crowell.com

Laurence Winston

Partner – London
Phone: +44.20.7413.1333
Email: lwinston@crowell.com

Lee Matheson, CIPP/US/E/A, CIPM, PCIP

Associate – Washington, D.C.
Phone: +1 202.654.6728
Email: lmatheson@crowell.com