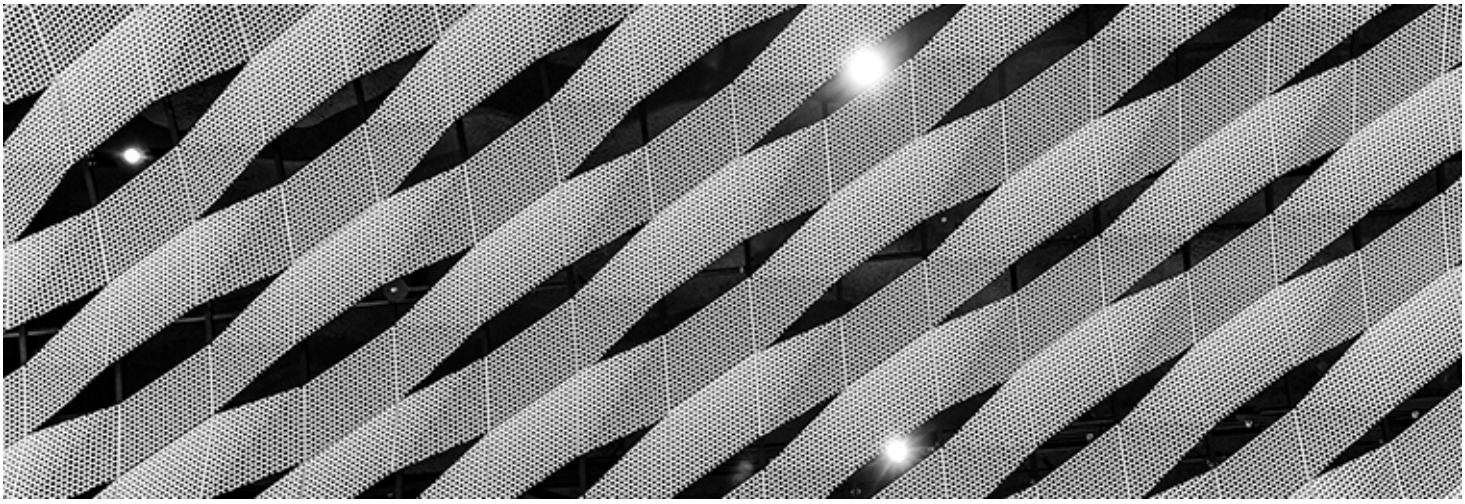

EU's highest court invalidates the EU-US Privacy Shield; European Standard Contractual Clauses remain valid, but subject to conditions

Data Protection, Privacy and Security Alert

16 July 2020
By: Carol A. F. Umhoefer | Katie Lee | Andrew Serwin

The Court of Justice of the European Union (CJEU) on July 16, 2020 handed down its long-awaited decision in the so-called *Schrems II* case (*Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18). In one of the most anticipated decisions of the year, the CJEU declared invalid the EU-US Privacy Shield framework for the transfer of personal data from the EU to the US. The CJEU also held that the Standard Contractual Clauses approved by the European Commission (commonly referred to as Model Clauses) remain valid subject to the requirement that businesses verify whether the conditions of transfer – including the destination country – offer appropriate safeguards to individuals' personal data in accordance with the GDPR.

Despite the uncertainty created by *Schrems II*, Standard Contractual Clauses currently remain the most realistic option for the transfer of personal data subject to GDPR. The full practical implications of the CJEU's decision will become more apparent in the coming days and weeks.

Background

The transfer of personal data subject to GDPR outside the EU is permissible if the requirements of GDPR Chapter V are satisfied. Permissible transfer mechanisms include adequacy decisions of the European Commission, such as Privacy Shield, or appropriate safeguards, such as Standard Contractual Clauses (SCC) or Binding Corporate Rules (BCRs).

This is not the first time the CJEU has invalidated an adequacy decision in favor of the US: In 2015, the CJEU invalidated the EU-US Safe Harbor framework (the predecessor to Privacy Shield) in the *Schrems I* case (see here). At the heart of plaintiff Schrems' complaint in both cases was the allegation that US surveillance laws do not offer adequate protection for personal data protected by EU laws, particularly in relation to Facebook's sharing of EU personal data with the US National Security Agency, a federal intelligence agency.

Key points of the CJEU judgment

In *Schrems II*, the CJEU has held that:

1. **Privacy Shield is no longer a valid mechanism for transferring personal data to US entities that have adhered to the Privacy Shield principles.** The CJEU has held that, due to the potential access to, and use by US public authorities of, personal data transferred to the US, a level of protection essentially equivalent to that guaranteed under EU law cannot be guaranteed. As summarized by the CJEU in its press release: *"[R]equirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country."* The CJEU has also held that the Privacy Shield Ombudsperson mechanism for affording redress to individuals does not provide an adequate level of protection because individuals do not have any cause of action before a body that offers guarantees substantially equivalent to those required by EU law.

2. **The SCCs continue to be a valid mechanism for transferring personal data to countries outside the EEA, but subject to limitations**. While the CJEU did not avail itself of the opportunity to invalidate SCCs, it held that SCCs may not always constitute a sufficient means of ensuring, in practice, the effective protection of transferred personal data, in particular *"where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates."* The judgment reiterates the importance of businesses verifying, prior to any transfer, whether an appropriate level of protection is respected in the recipient country. Where there are inadequate safeguards, the transfer of personal data to that country should be suspended by the EU exporter or, failing that, the relevant member state data protection authority. Although not explicitly referenced in the judgement, this reasoning would also apply to other appropriate safeguards, including BCRs.

What does this mean for US businesses?

The *Schrems II* decision has serious implications for the transfer of personal data outside the EU.

- Businesses should analyze data flows that involve transfers of personal data governed by GDPR outside the EU and determine which transfer mechanism (*eg*, Privacy Shield, SCCs) is purported to be used.
- For those transfers relying upon Privacy Shield, an alternative transfer mechanism must be found as a priority.
- For businesses currently using or considering using (as an alternative to Privacy Shield) SCCs, businesses must assess the level of appropriate safeguards provided by that transfer to determine whether SCCs are an available mechanism. This assessment should include consideration of the sector, industry, the destination country, the identity of the recipient and any other relevant factors – an assessment that may be challenging given the uncertainty in the CJEU's judgment in relation to relying on SCCs for transfers of personal data to the US.
- EU data protection authorities will have the unenviable task of ultimately determining the sufficiency of appropriate safeguards.
- The implications of the judgment are likely to trigger a further round of political discussions between the EU and US, with possible impacts on trade negotiations.

Given the impact this decision will have on businesses, we expect member state data protection authorities may

delay commencing enforcement actions to enable businesses time to assess their transfers and implement alternative solutions, as happened following the invalidation of the Safe Harbor framework by *Schrems I*. However, a grace period is not guaranteed and would not prevent individuals or groups from bringing private claims for compensation.

DLA Piper is developing a methodology to assist its clients in navigating the impact of the judgment and carrying out an assessment when relying on SCCs. For further information and advice, please get in touch with your usual DLA Piper contact.

AUTHORS

Carol A. F. Umhoefer
Partner
Miami | T: +1 305 423 8500
carol.umhoefer@dlapiper.com

Katie Lee
Associate
New York | T: +1 212 335 4500
katie.lee@dlapiper.com

Andrew Serwin
Partner
San Diego (Golden Triangle) | T: +1 858 677 1400
andrew.serwin@dlapiper.com