Data Transfer Turmoil: In Schrems II, Europe's Top Court Invalidates Privacy Shield And Casts Doubt On U.S. Companies' Ability To Rely On Standard Contractual Clauses

July 22, 2020

- While invalidation of the Privacy Shield is significant, the Court's holding concerning Standard Contractual Clauses may be more consequential for the many US companies that rely on them.
- The Court confirmed the general validity of SCCs for transferring data outside of the EU, but held that use of SCCs, without more, will not always be an adequate safeguard, particularly when the data importer is in the US or another country that gives law enforcement expansive surveillance powers.
- US companies, particularly those in certain regulated industries, should re-assess the safeguards they rely upon for each EU data transfer relationship and consider whether changes to safeguards, or the transfers themselves, are warranted.

What Happened?

Last week, the Court of Justice of the European Union ("CJEU") invalidated the EU-US Privacy Shield framework but gave qualified validation of EU Standard Contractual Clauses for the transfer of personal data to recipients outside the EU. The decision, in Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (known as "Schrems II"), contains significant implications for US companies that need to process personal data in compliance with the EU's General Data Protection Regulation ("GDPR").

The GDPR prohibits transfer of personal data to third parties outside of the EU unless the European Commission (the EU's executive branch) has deemed the recipient country's data protection laws "adequate," or the transfer is subject to some other form of "appropriate safeguards." Because the European Commission has not blessed the US with an adequacy decision, many US companies rely on Privacy Shield (a self-certification framework approved by US and EU authorities that is enforced by the Federal Trade Commission) or Standard Contractual Clauses (model clauses for the contract between the data "exporter" and data "importer" that have been approved by the European Commission) as their appropriate safeguards for data transfers.

Schrems II began as a dispute about the adequacy of SCCs for transfers of data to the US, but the Privacy Shield also became at issue as the case wound through the EU regulatory and judicial processes. Schrems challenged Facebook's use of SCCs at the end of 2015, when he updated an earlier complaint on the same data transfer issue related to US government mass surveillance practices with Ireland's data watchdog. He asked the Irish Data Protection Commission to suspend Facebook's use of SCCs. Instead, the regulator decided to take him and Facebook to court, saying it had concerns about the legality of the whole mechanism. In the wake of the CJEU's previous decision to overturn the Safe Harbor framework (the predecessor to Privacy Shield), Facebook had switched to SCCs as a way to legitimize their international transfers of EU personal data. Around the same time,

the European Commission agreed to replace Safe Harbor with the Privacy Shield. When the case was referred to the CJEU, the questions posed to the Court were expanded to include consideration of the wider issue of EU-US data transfers more generally, including the validity of Privacy Shield.

With respect to the Privacy Shield, the CJEU found that "the requirements 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", and that mechanisms in the EU-US Privacy Shield ostensibly intended to mitigate this interference are not up the required legal standard of 'essential equivalence' with EU law. In particular, the CJEU found that the Privacy Shield's Ombudsperson mechanism does not provide substantially equivalent guarantees to those required by EU law, questioning its independence and lack of authority to make binding decisions on U.S. intelligence services.

With respect to SCCs, the CJEU reaffirmed their validity but stated that companies must verify, on a case-by-case basis, whether the law in the recipient country ensures adequate protection, consistent with EU law, for personal data transferred under SCCs. Where the laws of the recipient country don't offer adequate protection, the data exporter and importer must implement other safeguards, in addition to SCCs, or suspend transfers altogether.

So what does this mean?

Companies that until now have relied on the EU–US Privacy Shield for data transfers from the EU to the US must implement alternative safeguards. Instead of relying on the Privacy Shield, companies can consider several options, outlined under Article 46 of the GDPR, including binding corporate rules, which must be approved on a company-by-company basis by EU data protection authorities and, while left out of the decision, are presumably now subject to similar limitations. Or, companies can still use SCCs, but must re-assess their adequacy for each particular data transfer relationship.

While the CJEU outlined this new requirement for SCCs, it did not provide any guidance on what additional safeguards might look like in instances where the recipient country's laws are inadequate. The European Commission declared that it is working on alternative instruments for international transfers of personal data, including by reviewing the existing SCCs. But in the case of third countries that permit law enforcement broad surveillance powers, it's not clear how data exporters are capable of implementing additional safeguards that could pass muster under Schrems II, since law enforcement isn't bound by contractual protections imposed on data importers.

What should US companies do?

One potential way to continue using SCCs is to demonstrate that some categories of data transferred and some data recipients are not subject to US surveillance laws. For example, Omer Tene, Vice President and Chief Knowledge Officer at the International Association of Privacy Professionals, noted that "US Foreign Intelligence Surveillance Act Section 702, Executive Order 12333 and Presidential Policy Directive 28 concern communication service providers, not retailers, manufacturers, health care or pharma companies, or the thousands of companies that use SCCs to export employee data to headquarters in the U.S. This means that the vast majority of companies can use SCCs in transfers to the US" without material changes. However, this theory is thus far untested and it is unclear whether EU authorities would agree that SCCs are always sufficient, without more, in all the contexts Mr. Tene described. Moreover, companies that transfer contents of communication such as telecommunication and cloud providers or companies using services by such providers would likely be unable to make the argument Mr. Tene posits.

In conclusion, companies that are currently relying on the Privacy Shield for data transfers will have to reconfigure that approach. For companies relying on SCCs, they will have to consider, on a case by case basis,

what additional safeguards may be necessary to ensure an "adequate level of protection." Companies are at risk if they continue to simply incorporate SCCs into their data processing agreements without scrutinizing their adequacy in the context of each data transfer relationship.

Authors:

Travis P. Brennan
949.725.4271
tbrennan@sycr.com

Katie Beaudin
949.725.4074
kbeaudin@sycr.com