Proskauer

One Cross-Border Mechanism Invalid, Another Upheld: Thoughts after the CJEU's Schrems II Decision

Proskauer on Privacy Blog on **July 21, 2020**

On July 16, 2020, the Court of Justice of the European Union (CJEU) invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield, ruling, among other things, that U.S. domestic law governing law enforcement access to transferred data does not satisfy the GDPR's requirements because, as the Court stated, U.S. surveillance programs are not limited to "what is strictly necessary to achieve the legitimate objective in question". In a separate portion of the opinion, however, the CJEU upheld as valid Commission Decision 2010/87 on standard contractual clauses (SCCs) for the transfer of personal data to processors established in third countries. This is the second ruling (known commonly as "*Schrems II*") by the CJEU overturning an established mechanism to transfer personal data from the EU to the U.S. Indeed, only five years ago the CJEU issued its "*Schrems I*" decision invalidating the long-standing EU-U.S. Safe Harbor, which had been a method to transfer data across the Atlantic without running afoul of the EU Data Protection Directive, a predecessor of the GDPR.

As it stands, *Schrems II* jeopardizes the flow of data from Europe to the U.S. and businesses now face a similar situation to 2015 when a favored mechanism to transfer personal data was similarly invalidated. Not surprisingly, alarmed reactions came from the U.S., including two U.S. Senators calling the decision "troubling" and economically disruptive, the U.S. Commerce Dept. Secretary calling it "deeply disturbing," with all officials hoping that negotiators can quickly hammer out a successor framework.

The *Schrems* Rulings

In 2015, in the wake of the *Schrems I* decision, the European Commission adopted the EU–U.S. Privacy Shield, a framework designed to replace the invalidated EU-U.S. Safe Harbor program. The *Schrems I* court had ruled that the Safe Harbor program did not adequately protect personal data from "interference" from the U.S. government "founded on national security and public interest requirements" (note: The *Schrems I* challenge was spurred by the Edward Snowden leak about certain U.S. government PRISM program and other digital surveillance practices involving individuals' personal data and communications). At that time, the Privacy Shield was designed as a "robust new system" that would allow U.S. companies to meet stronger obligations to protect Europeans' personal data, with the Department of Commerce and FTC engaging in stricter monitoring and enforcement and the government appointing a Privacy Shield Ombudsperson. As the *Schrems* case–brought by an Austrian privacy activist–continued to wend its way through European courts, it made its way again to the EU's highest court, and here are we again in 2020 facing the same outcome.

The purpose of the European Commission's adequacy decision backing the Privacy Shield is to find that the third country (in this case, the U.S.) ensures a level of protection to personal data essentially equivalent to that imposed under EU law. The adoption of an adequacy decision assumes that the Commission had evaluated the level of protection guaranteed by the law and the practices of that third country in the light of the various factors set out in Article 45 of the GDPR. One of these considerations includes the legislation of the third country relating to national security and surveillance. The CJEU reasoned that, under the GDPR, the adequacy decision must ensure that the rights of the persons whose data are transferred, "benefit…from a level of protection essentially equivalent to that which follows from the GDPR." In *Schrems II*, the CJEU invalidated the adequacy decision for the Privacy Shield for a number of reasons, principally concerning the extent of U.S. government surveillance permitted under the Foreign Intelligence Surveillance Act (FISA) law. The Court noted, among other things, that the U.S. government's surveillance programs do not have adequate limitations and the EU Privacy Ombudsperson and other agencies do not otherwise offer comparable remedies for potentially targeted EU persons.

In another part of its judgment, however, the CJEU validated SCCs, another mechanism to transfer data from the EU to the U.S. The Court noted, among other things, that the SCCs provide for enforceable rights and remedies against the exporter and, in the alternative, against the importer, and that supervisory data protection authorities possess corrective powers that can be used to issue warnings to noncompliant controller, or in some cases, impose a temporary or definitive limitation or ban on processing. Despite declining to invalidate the SCCs, the court suggested certain obligations for the data importer and exporter, namely that a controller established in the EU and the recipient of personal data are **"required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned."** The Court added that: "The recipient is, where appropriate, under an obligation…to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract."

Final Takeaways

So, where does that leave the over 5,000 businesses that had been enrolled in the Privacy Shield program? The potential disruption is significant. At this time, there has been no official word from EU officials about a grace period for companies using the Privacy Shield to transition its data transfer practices (as had occurred following the invalidation of the EU-U.S. Safe Harbor). In fact, the Berlin data protection authority issued a statement following *Schrems II* and stated that data controllers in Berlin storing personal data in the U.S. should return such data to Europe. The official also emphasized that data importers in third countries are obliged to check before the first data transfer whether there is state access to the data in the third country that goes beyond what is permitted under the GDPR. Thus, it is incumbent on companies relying on the Privacy Shield framework or those that contract with vendors that rely on the Privacy Shield to immediately reassess and implement other data transfer mechanisms identified in the GDPR. Though more burdensome than self-certifying under Privacy Shield, companies might choose to use binding corporate rules and the aforementioned standard contractual clauses to process legal data transfers. Still, even for those entities relying on SCCs, their work is not done. Entities who rely on SCCs should be prepared for questions and risk assessments from data exporters to non-EU data importers regarding whether the companies are complying with the SCCs and offering adequate levels of protection. Beyond these issues, there are questions regarding data transfers between the UK and U.S. (for the time being, the UK is under a transition period until the end of the year and the UK data protection authority has stated that its government intends to incorporate the GDPR into UK data protection law from the end of the transition period). Also, an interesting question has arisen whether California could apply for an adequacy decision based upon the protections afforded under the CCPA. As we learned with the invalidation of the Safe Harbor, this will be an ongoing process, with conditions changing as negotiators from both sides attempt to forge a new compromise that complies with EU law and will survive a court challenge. We will continue to follow developments closely.

Special thanks to Jonathan Mollod for his significant contribution to the blog post.

View Original