Transferring Personal Data To US After EU Top Court Ruling

By **Natasha Kohne, Michelle Reed and Jenny Arlington** (July 20, 2020)

Natasha Kohne

Michelle Reed

Jenny Arlington

On July 16, the Court of Justice of the European Union handed down its highly anticipated judgment in a case brought by privacy activist Max Schrems.[1]

The case concerned transfers of personal data of European Union citizens outside the EU under the General Data Protection Regulation. One of the mechanisms for transfer to the U.S., the EU-U.S. Privacy Shield, was invalidated by the CJEU. Another mechanism, the use of standard contractual clauses, or SCCs, was in principle upheld, but the CJEU explained that the SCCs can be relied on only in certain circumstances.

A bold question mark was put on whether the SCCs could be used for personal data transfers to the U.S. The issue that faces data controllers and processors now is how to transfer personal data to the U.S. in compliance with the GDPR. The answers seem to be in the making.

What Was Schrems II About?

Schrems is a known figure in the data privacy circles. He was the main actor behind the complaint that led to the CJEU's decision invalidating the safe harbor, another mechanism under which companies could transfer personal data from the EU to the U.S., in 2015.

Schrems' renewed challenge in Schrems II was against the SCCs, in particular the SCCs on which Facebook Ireland Ltd. relied for transferring a large part of the personal data of EU-based users to Facebook Inc. in the U.S. Schrems maintained that U.S. law required Facebook to make such data available to certain U.S. authorities, including the U.S. National Security Agency and Federal Bureau of Investigation, which he asserted was incompatible with his data privacy and other fundamental rights.

The Irish Data Protection Commissioner, or Irish DPC, investigated Schrems' complaints and issued an interim draft decision, stating that it would likely find that the personal data of EU citizens would be processed by the U.S. authorities in a manner incompatible with Articles 7 — respect for private and family life — and 8 — protection of personal data — of the Charter of Fundamental Rights of the European Union. The Irish DPC also preliminarily found that U.S. law did not provide EU citizens with legal remedies compatible with Article 47 — the right to an effective remedy and to a fair trial — of the charter.

The CJEU was then asked to consider 11 questions in relation to what the GDPR, the charter and other EU laws allow as regards personal data transfers outside the EU, in particular to the U.S.

SCCs Confirmed as Valid, But Only Where Compliance with Them Can Be Achieved in Practice

The CJEU was asked whether a data protection authority, or DPA, is required to suspend or

prohibit a transfer of personal data to a third country pursuant to SCCs, if the DPA's view is that the SCCs cannot be complied within that third country. The short answer is yes, it is. The CJEU explained that if the European Commission has made an adequacy decision — currently issued to only 12 jurisdictions — that is still in place, a DPA cannot validly conclude that a jurisdiction does not offer adequate protection.

However, for all the other third countries where no commission adequacy decision is in place, a DPA is allowed to take a view that the SCCs are not, or cannot be, complied with, and that EU law requirements for the protection of the data transferred cannot be ensured by other means.

The CJEU ruled that, in such cases, the DPA must suspend or prohibit the transfer, unless the controller or the processor have already done so. Faced with the risk that the DPAs in each member state can adopt divergent decisions, the CJEU reminded DPAs of the possibility to refer the matter to the European Data Protection Board so that it can adopt a binding decision applicable to all member states.

The CJEU also examined whether SCCs should be invalidated, given that they are in place where there is no commission adequacy decision and, by their contractual nature, do not bind the authorities in third countries. The CJEU, like the advocate general, found that there is nothing to affect the validity of the legal instrument with which the SCCs were put in place.

However, the CJEU emphasized that their validity depends on whether in practice the SCCs make it possible to ensure compliance with the level of protection required by EU law, as envisaged by the various rights and obligations in the wording of the SCCs. In the event of a breach of the SCCs or impossibility to honor them, the transfer should be suspended or prohibited.

The CJEU pointed out the EU data exporter's obligation to consider the country-specific data protection laws and other legal requirements before entering into SCCs and suspend the data transfer or terminate the contract where the recipient outside the EU is not, or no longer able, to comply with the obligations under the SCCs.

The court also reminded companies of the duty of the U.S. recipient of personal data to inform the EU counterparty about any inability to comply. The CJEU also suggested that controllers and processors relying on the SCCs may need — and are indeed encouraged — to adopt supplementary measures and conduct due diligence prior to entering into SCCs.

Privacy Shield Invalid Immediately

In addition to reviewing the SCCs, the CJEU reviewed the validity of the Privacy Shield which was a framework arrangement that allowed the transmission of personal data from EU entities to certified U.S. entities. The CJEU ruled that the Privacy Shield was invalid with immediate effect.

First, the CJEU found that a derogation in the Privacy Shield Framework Principles issued by the U.S. Department of Commerce enabled interference with personal data based on national security, public interest or on the basis of U.S. domestic legislation. Those limitations on the protection of personal data arising under domestic U.S. law were not equivalent to the limitations allowed under EU law.

In particular, the CJEU examined Section 702 of the Foreign Intelligence Surveillance Act,

Executive Order 12333 and Presidential Policy Directive 28, and concluded that none of them contain any restrictions on the power to implement surveillance programs for the purposes of foreign intelligence, and none of them contained any safeguards for non-U.S. persons potentially affected by such programs.

Second, the CJEU explained that Article 47 of the charter required data subjects whose rights and freedoms were guaranteed by EU law to have an effective remedy before a tribunal. Data subjects were not granted rights actionable in the courts against U.S. authorities and thus had no right to an effective remedy in relation to surveillance programs based on Section 702 of FISA or EO 12333.

The CJEU held that the introduction of an ombudsperson did not remedy the deficiencies, because, among other things, the ombudsperson was an integral part of the U.S. State Department and hence not independent.

Reactions of Regulators and Institutions So Far

The judgment has already caused waves in the data privacy world and will be the subject of many ongoing discussions. Some of the regulators, members of the commission and governments have already issued statements addressing the immediate aftermath. There have been indications that further detailed guidance would be forthcoming.

The European Data Protection Board noted that, with regard to privacy shield, it would continue assisting the commission in securing, together with the U.S., a transatlantic transfer mechanism that would fully comply with EU data protection law. The European Data Protection Board also stated that it was looking into guidance as to what additional measures data exporters could put in place when entering into certain SCCs.

The EU Commissioner for Justice Didier Reynders announced immediately after the judgment that it would be very important to start the process to have formal approval to modernize the SCCs as soon as possible. The SCCs have not yet been updated since the GDPR.

The approaches by the DPAs in the aftermath of Schrems II are divergent. Some have been vocal in their support for the judgment. For example, the Irish DPC noted that it "strongly welcomes" the decision and that it had commenced the proceedings in 2016 "precisely because it was concerned that … EU-U.S. data transfers were inherently problematic … whatever the legal mechanisms by which such transfers were conducted."

The Berlin DPA went even further and announced that all personal data transfers to the U.S. should be suspended, stating: "Now is the hour for Europe's digital independence."

Other DPAs have been more cautious. The U.K. Information Commissioner's Office stated that it was reviewing the judgment and would stand ready to support U.K. organizations. The U.K. government also issued a statement, saying it was "disappointed" that the privacy shield was invalidated.

What Should Companies Do Now?

The invalidation of the privacy shield and the qualifications of when SCCs can be relied upon leave significant questions for controllers and processors who transfer data from the EU to third countries, in particular to the U.S.

Much of what happens next depends on further guidance by the regulators and political steps in relation to implementation of new frameworks or changes to existing U.S. laws. Looking ahead, at this stage controllers and processors should consider the following:

1. Review current transfer mechanisms.

Companies relying exclusively on the privacy shield for transfers of data from the EU to the U.S. should examine their position and consider what alternative mechanisms they could rely on in order to transfer personal data lawfully to the U.S. The CJEU ruling does not have a grace period so its effect is immediate.

In light of the reasons identified by the CJEU as to why the privacy shield, and previously the safe harbor, are invalid, we suspect that a further version of a similar framework, if at all possible, will take some time.

At the same time, importantly, U.S. companies that currently participate in privacy shield must remain compliant as the Department of Commerce will continue enforcing privacy shield, stating that the "decision does not relieve participating organizations of their Privacy Shield obligations."

2. Review the status of SCCs and compliance efforts.

In light of the Irish DPC's preliminary finding that the U.S. does not offer an adequate level of protection, statements by several DPAs and the CJEU's ruling that in circumstances where such finding exist the transfer must be suspended or terminated, we anticipate increased scrutiny on companies relying on SCCs for transfer of personal data to the U.S.

Transfers to other third countries under the SCCs should be examined on a case-by-case basis, preferably by the exporters of data before the relevant DPA starts an investigation. At a minimum, companies should be prepared to show that the provisions of the SCCs are being adhered to and companies should consult with legal counsel on additional measures to enhance protection.

3. Consider other transfer mechanisms and additional safeguards.

Other transfer mechanisms such as derogations under the GDPR should be considered. Binding corporate rules might also be a possibility, although there is a risk that the concerns raised by the CJEU as regards transfers to the U.S. would impact this mechanism as well. To the extent that SCCs must be relied upon, companies should consider country-specific data protections laws and determine whether any additional safeguards can be included in the SCCs for that specific transfer.

4. Pay attention to statements and guidance from the regulators in each EU member state.

As noted above, the various DPAs are already having somewhat diverging opinions. We anticipate that the European Data Protection Board will be asked to harmonize the approach in relation to transfers of data to the U.S. The U.K.'s position will be closely watched once it leaves the EU at the end of this year.

Natasha Kohne is a partner and co-head of the cybersecurity, privacy and data protection

practice Akin Gump Strauss Hauer & Feld LLP.

Michelle Reed is a partner and co-head of the cybersecurity, privacy and data protection practice at the firm.

Jenny Arlington is counsel at the firm.

Akin Gump associate Rachel Kurzweil and trainee solicitor Sahar Abas contributed to this article.

[1] C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems ("Schrems II"), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9793916.