July 30, 2020

ARTICLE

“Schrems II”: Impacts on agreements involving processing personal data outside the EEA

On July 16, 2020, the Court of Justice of the European Union (CJEU) issued its judgment in case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* (the Schrems II Decision). The judgment invalidates the EU-U.S. Privacy Shield adequacy decision from the European Commission (the Privacy Shield Decision). It also requires EU data exporters relying on the European Commission’s Standard Contractual Clauses to transfer personal data to any third country to verify, prior to undertaking such transfer, that the level of protection granted by the recipient in such country will be adequate.

One week later, the European Data Protection Board (EDPB) issued a Frequently Asked Questions document on the Schrems II Decision (the FAQ), which clarifies some of the consequences regarding processing arrangements that involve reliance on the Privacy Shield, Standard Contractual Clauses, Binding Corporate Rules and the EU’s General Data Protection Regulation (GDPR) Article 49 derogations.

Below, we summarize some key the effects of the Schrems II Decision and its immediate impact for organizations processing personal data outside of the European Economic Area (EEA). The EDPB is expected to issue further guidance shortly, and the European Commission indicated it is working closely with its U.S. counterpart to find an alternative to the Privacy Shield, to provide a strengthened and durable transfer mechanism.

1. The Privacy Shield is invalid

In light of the requirements set forth in the GDPR, the Court examined the validity of the Privacy Shield.

It concluded that domestic U.S. laws regulating access and use by its public authorities of personal data for national security purposes (namely FISA Section 702 and EO 12333) interfere to such an extent with the fundamental rights of EU data subjects that the Privacy Shield Decision cannot ensure a level of protection “essentially equivalent” to the one required under EU data protection law. The Court also highlighted that the lack of effective judicial redress available to EU data subjects in the context of U.S. intelligence programs violates EU data protection law. Consequently, the CJEU invalidates the Privacy Shield, effective immediately.

2. SCCs remain a valid transfer mechanism, but require new diligence from the data exporter and importer

In its judgment, the CJEU also examined the validity of the European Commission’s Decision 2010/87/EC on Standard Contractual Clauses for the transfer of personal data to processors established in third countries (SCCs) and considered that transferring personal data pursuant to such mechanism remains lawful to the extent that it is possible for the parties, in practice, to (i) ensure compliance with a level of protection essentially equivalent to that guaranteed within the EU by the GDPR; and (ii) to suspend or prohibit transfers in the event of the breach of such clauses or it being impossible to honour them.

Organizations commonly rely on SCCs to transfer personal data. Hence, the Court’s conclusion impacts a large number of transfers (including subsequent transfers to sub-processors) of personal data to non-adequate jurisdictions, *i.e.* not only to importers located in the U.S.

In that regard, the Court highlighted the existing obligation of both the data exporter and importer to verify, prior to any transfer, and taking into account the circumstances of the transfer, whether the level of protection required by the GDPR is respected in the third country. Further, the data importer must inform the data exporter of any inability to comply with the SCCs, and, where necessary, with any supplementary measures adopted contractually by the parties to ensure an adequate level of protection, the data exporter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the data importer. Failing that, the competent Supervisory Authority is required to intervene should the parties decide to nontheless proceed with the transfer.

The EDPB indicated in its FAQ that it is currently analysing the Court’s judgment to determine the type of supplementary measures that could be provided by the parties to a data transfer to a non-adequate jurisdiction, which could be legal, technical and/or organisational, to provide a sufficient level of protection. Further guidance on this point will be crucial to ensure compliance with the GDPR.

3. Impact on agreements involving the processing of personal data outside the EEA

In its judgement, the Court found that U.S. law infringes the fundamental rights of data subjects. This conclusion may trigger modifications to U.S. law, which has been under increased scrutiny since Edward Snowden’s revelations. In the meantime, organizations transferring personal data as well as organizations located in the U.S. and in other jurisdictions that are not recognized by the European Commission as providing an adequate level of protection must take note of the Schrems II Decision, and consider the following operational impacts:

International transfers relying on the Privacy Shield

The CJEU invalidated the Privacy Shield adequacy decision without granting a grace period for ongoing transfers to companies certified under the Privacy Shield program. From an EU law perspective, organizations relying on this transfer mechanism to send personal data to the U.S. should immediately cease such transfers, unless they can rely on another mechanism under Chapter 5 of the GDPR.

Given the current state of U.S. law regarding state surveillance (which overrides contractual arrangements such as SCCs or BCRs), there is uncertainty as to whether data transfers to the U.S. can be legitimized, unless the parties can ensure an adequate level of protection by using the SCC complemented with supplementary measures (see below) or if they meet one of the derogations provided under Article 49 of the GDPR (*i.e.* consent of the data subject, transfer necessary for the performance of a contract between the data subject and the controller or transfer necessary for important reasons of public interest). At this point and considering the current COVID-19 crisis, it appears unlikely that a new framework will be adopted by the EU and the U.S. prior to the U.S. presidential elections in November.

International transfers relying on Standard Contractual Clauses

Whether or not an organization can transfer personal data outside of the EEA on the basis of SCCs (whether to a third party or to an affiliate) will depend on the result of its risk assessment, taking into account the circumstances of the transfer on a case-by-case basis and supplementary measures it could put in place with the recipient of the data.

The supplementary measures, along with SCCs (SCC+), should ensure compliance with a level of protection essentially equivalent to that guaranteed within the EU by the GDPR and make it possible in practice for the parties to suspend or terminate the transfer in case of a breach of those contractual arrangements ,or if the recipient cannot honour them. They would also have to ensure that the law the data importer (*i.e.* the processor) is subject to does not infringe on the adequate level of protection they guarantee. As mentioned above, the EDPB is currently analysing the Schrems II Decision, and has indicated that it will provide further guidance regarding what those supplementary measures could be. It should also be noted that the European Commission is currently working on a new set of SCCs, which will hopefully provide for such measures, in addition to fixing the deficiencies of the current sets of clauses.

However, if taking into account the circumstances of the transfer (and supplementary measures, as the case may be), the data exporter concludes in its risk assessment that appropriate safeguards would not be ensured, it is required to suspend or end the transfer of personal data. If the exporter intends to keep transferring data despite this conclusion, it must notify its competent Supervisory Authority.

Parties who have traditionally entered into SCCs as a template document, without really assessing their legal effects, must therefore pay greater attention to their detailed requirements and carefully assess whether the processing they contemplate provides an adequate level of protection once the data is received by the data importer located in a third country.

Depending on the outcome of such assessment, the parties may enter into the current SCC or the SCC+. The data exporter may also decide not to proceed with the contemplated transfer if the level of risk is too high, or proceed with the transfer after notifying its Supervisory Authority.

International transfers relying on Binding Corporate Rules

The Court's assessment and above analysis also applies in the context of BCRs, since the law of the country where the data importer is located will similarly have primacy over this tool. The EDPB's expected additional guidance will likely cover the validity of BCR as a transfer mechanism to third countries and possible supplementary measures as necessary.

By: Elisa Henry

Services: Cybersecurity, Privacy & Data Protection, Online Retail & E-commerce

---