CLIENT ALERT

The European Commission's Standard Contractual Clauses: Good News from the Advocate General, but We're Not Out of the Woods

Jan.08.2020

Standard Contractual Clauses (SCCs), as established by the European Commission, have long been used to safeguard personal data transferred outside the European Union (EU). But the companies that typically use SCCs need to be aware that they no longer provide the solid data transfer mechanism that they used to.

While organizations have been updating their policies and procedures to meet the requirements of the General Data Protection Regulation (GDPR), the SCCs are stuck in a pre-GDPR era, which gives them an outdated look and feel. But what is worse, their validity has been questioned and is now being examined by the highest European court. This could lead to their immediate invalidation, or even to the conclusion that they have never been valid at all.

So a lot is at stake for the SCCs, and more specifically those used by non EU-based processors, in the *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) case – more commonly referred to as 'Schrems II'.

The good news is that the Advocate General (AG) issued its opinion on December 19, 2019, and the AG found nothing to affect the validity of these SCCs.

While this opinion is highly authoritative, it is not binding on the Court however. As a result, the legal uncertainty over the status of SCCs continues for now. This situation is not only detrimental for the position of the EU in the global digital economy, but truly frustrating for organizations that just want to be compliant with the EU's strict data protection legislation.

Moreover, the AG found that SCCs are not in themselves sufficient to provide adequate protection, and should not be relied upon if there is a conflict with the law of the third country in question that precludes compliance with the SCCs. Thus, even if the validity of the SCC's is ultimately confirmed, data controllers and, where they fail to act, supervisory authorities, should suspend or prohibit a transfer when, because of a conflict between the law of the third country and the obligations of the SCC's, the SCC's cannot or can no longer be complied with.

The Background

Under the General Data Protection Regulation (GDPR), personal data may be transferred to a third country if that country provides an adequate level of protection for the personal data; the assessment of the country's level of protection is done by the European Commission (EC) and made concrete in a formal 'adequacy decision.'

However, the EC also allows data to be transferred to third countries without an adequacy decision if there are appropriate safeguards in place. And in February 2010 the EC created a mechanism for meeting this requirement by approving SCCs for the transfer of personal data to processors established in third countries. The SCCs were considered to offer adequate safeguards

with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights required by Article 26(2) of the – then still valid – Data Protection Directive 95/46/EC.

The Facts – Another Chapter in the Schrems Privacy Saga

In 2013, Mr. Maximillian Schrems objected to his data being sent by Facebook Ireland to servers in the U.S., arguing that, in light of the 2013 revelations made by whistleblower Edward Snowden, personal data does not receive adequate protection in the U.S. Facebook argued that the data was protected under the 'Safe Harbour' mechanism established by the EC in an 'adequacy decision,' allowing transfers to U.S. data importers that complied with the scheme.

As a result of Schrems' complaint (Schrems I), the EC decision establishing the Safe Harbour scheme was invalidated by the Court of Justice of the European Union (CJEU), *i.e.,* the same court that is considering the case at hand. The Safe Harbour scheme was subsequently replaced by the EC's "EU-U.S. Privacy Shield" decision, a similar scheme that considers the U.S. to provide an adequate level of protection of data transferred to the U.S. under the Privacy Shield system.

In a 2018 follow-up complaint (Schrems II), Mr. Schrems targeted the validity of SCCs and the EC decision establishing them.

Before the Court issues a ruling, the parties have the opportunity to submit their written and oral observations, after which the Advocate General (AG) issues his opinion. The hearing took place on July 9, 2019 and the AG's opinion was released on December 19, 2019.

The AG's Opinion

AG Henrik Saugmandsgaard Øe concluded that analysis of the questions for a preliminary ruling has disclosed nothing to affect the validity of the SCC's. He advised the CJEU to rule that the

> analysis of the questions for a preliminary ruling has disclosed nothing to affect the validity of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016.

Our interpretation of the 96-page opinion results in the following key take-aways:

1. EU law applies to the transfer of personal data for commercial purposes to a third country even if the data may be further processed by its authorities for national security purposes.
2. The SCCs provide a mechanism that applies irrespective of the third country in question and irrespective of the level of protection guaranteed there. Analysis of the questions for a preliminary ruling has disclosed nothing to affect the validity of the SCC's.
3. The SCCs are not in themselves sufficient to provide adequate protection, and should not be relied upon if there is a conflict with the law of the third country in question that precludes compliance with the SCCs. Data controllers and, where they fail to act, supervisory authorities, should suspend or prohibit a transfer when, because of such conflict between the law of the third country and the obligations of the SCC's, the SCC's cannot (or no longer) be complied with.

4. Although the referring court did not directly call into question the validity of the EU-U.S. Privacy Shield, the AG does question its validity, so that its future and the corresponding legal uncertainty remains.

Conclusion: Troubling Times Ahead for Transatlantic Data Transfers?

At first glance, the opinion of the AG may seem to be a victory for international data transfers, as it would be difficult to uphold the validity of other data transfer mechanisms if the EC Decision 2010/87/EU establishing the SCCs for processors were invalidated.

However, even in the event that the CJEU follows the AG's opinion and upholds the validity of SCCs as a data transfer mechanism, SCCs do not give carte blanche for data transfers to any third country. It will be the exporter's responsibility to assess whether the SCCs can be complied with and, in line with the GDPR's accountability obligation, to demonstrate that such assessment was carried out before the transfer in question.

As supervisory authorities are explicitly called out in the AG's opinion we can expect a closer scrutiny of supervisory authorities in this area.

Moreover, the EC will have to issue a new version of the SCCs that adapts them to the GDPR and will need to determine how the new versions will operate alongside the existing ones.

These trends, together with the doubts cast over the validity of the Privacy Shield, may yet be a recipe for some troubling times ahead in the field of transatlantic data transfers.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Maarten Stassen
Partner – Brussels
Phone: +32.2.214.2837
Email: mstassen@crowell.com

Frederik Van Remoortel
Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com

Jarno Vanto, CIPP/E, CIPP/US
Partner – New York
Phone: +1 212.803.4025
Email: jvanto@crowell.com