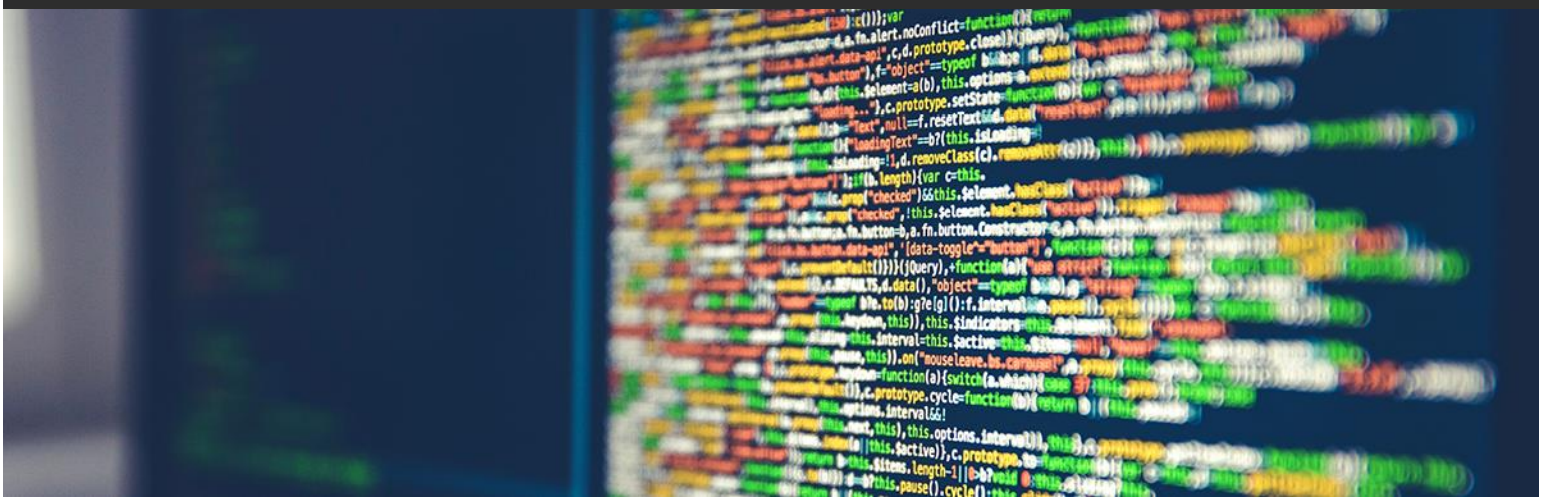
GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity



June 2021

EU Decision on Cross-Border SCC of June 4, 2021

On 04 June 2021, the EU Commission adopted two new sets of standard contractual clauses (SCC): one set for the transfer of personal data from the EU to third countries (Cross-Border SCC) and another set addressing certain clauses in controller-processor data processing agreements (DPA-SCC). The adoption was made some seven months after initial drafts of both SCC had been published by the EU Commission for public consultation (see GT blog post from 18 November 2020). *This GT Alert discusses the new Cross-Border SCC. The DPA-SCC will be addressed separately.*

First Things First: When do the new SCC enter into force and what does that mean?

The Cross-Border SCC become applicable on 27 June 2021. Until 27 September 2021, both the "old" SCC and the new SCC can be used for contracts; thereafter the old SCC may no longer be used for new contracts but will continue to be deemed "appropriate" for another 15 months as long as the subject matter of these contracts remains unchanged and provided that the old SCC were "appropriate" before. As of 27 December 2022, the use of the "old" SCC will no longer provide the necessary appropriate safeguards for a data transfer to a third country, and by then, they need to be replaced by the new Cross-Border SCC (or other appropriate means).

This means that (1) from 27 September 2021 onwards, only the new Cross Border SCC can be used for data transfers to third countries in new contracts, and (2) from 27 December 2022 onwards, all existing "old" SCC will need to have been replaced by the new SCC.

What are Cross-Border SCC and why are they important?

Under the EU General Data Protection Regulation (GDPR), personal data may only be transferred from the EU to a third country (i.e., a country that is not a member state of the European Economic Area, EEA) if appropriate safeguards are in place. For many years, one of the most popular mechanisms and easy-to-implement alternative for ensuring that appropriate safeguards were in place, were so-called standard contractual clauses for cross border transfers (the "old" SCC).

The "old" SCC were drafted under the GDPR's predecessor, the Data Protection Directive, and continued to be applicable until now. In July 2020, the Court of Justice of the European Union (CJEU) declared in its Schrems II ruling that undefined "supplementary safeguards" might need to be implemented for data transfers based on the old SCC without clarifying which "supplementary safeguards" might be necessary, or how to determine them. In November 2020, the European Data Protection Board (EDPB) published its draft "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" (Recommendations), providing organizations an assessment process for protecting EU personal data transfers. The new SCC are consistent with the GDPR and respond to the Schrems II ruling.

While the Cross-Border SCC offer some clarity, there are many challenges and hurdles that data exporters and data importers need to overcome when relying on Cross-Border SCC for data transfers in the future.

What transfers are covered by the Cross-Border SCC?

The new Cross-Border SCC follow a different structure than the "old" SCC. They apply a modular approach (for all varieties of transfers between controllers and processors) and offer the possibility that more than two parties join and use the Cross-Border SCC. But most importantly, the new Cross-Border SCC can be used for all types of data transfers, regardless of the legal "role" of the data exporter and the data importer (i.e., whether the exporter or importer is a controller or processor).

What are the key takeaways?

Against the initial draft from November 2020, the Cross-Border SCC have been amended substantially both in terms of language and substance. Also, the EU Commission adopted a number of recommendations from the EDPB/EDPS (see our GT Alert from November 12, 2020).

The key aspects of the new Cross-Border SCC include the following:

- In relation to the Schrems II ruling, the Cross-Border SCC allow organizations to take a risk-based approach when assessing the possibility of (foreign) public authorities accessing the data under their local laws. The parties must warrant in considerable detail, that they have no reason to believe the laws and practices in the third country applicable to the processing of the personal data by the data importer prevent the data importer from fulfilling its obligations under the Cross-Border SCC.
- The contractual parties must assess the general circumstances of the transfer (e.g., regarding the number of parties involved, the types of recipients, the purposes of processing and the categories of personal data transferred).
- The contractual parties must assess the laws and practices of the third country of destination "relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards". Unlike the EDPB's draft Recommendations that noted any assessment must not rely on subjective

factors, the new Cross-Border SCC provide that this analysis includes the evaluation of "practical experience with prior instances of requests for disclosure from public authorities".

- The parties' assessments must be documented, stored, and made available to the relevant supervisory authority upon request.
- The data importer must review the legality of all data disclosure requests made by public authorities, and must notify the data exporter of such requests, or even forward them to the data exporter. In cases of doubt, it must challenge the requests regarding their lawfulness.
- The Cross-Border SCC must describe the specific (i.e., not merely generic) technical and organisational measures to be implemented by the data importer which measures must ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons.
- Many of the provisions in the Cross-Border SCC confer rights to individuals that they are entitled to invoke although they are not a party to the underlying agreements, or the Cross-Border SCC.
- The Cross-Border SCC provide a termination right to the data exporter in case of certain breaches of the Cross-Border SCC.

What are the next steps?

Organizations should review the status of their international data transfers from the EU to a third country. As soon as possible, but in any event from 28 September 2021 onwards, they should only use the new Cross-Border SCC when entering into new contracts. In addition, they should replace any "old" SCC previously implemented, with the new Cross-Border SCC, such replacement to be finalised by 28 December 2022.

It is important to note that even with the new Cross-Border SCC, "supplementary measures" may be necessary, depending on the third country to which data is exported, and the business model / nature of the data importer, the ways the data is processed in the third country, etc. It is expected that the EDPB will release the final version of its Recommendations in mid-June, which will hopefully further clarify the circumstances when supplementary measures are necessary in cross-border transfers of EU personal data.

Authors

This GT Alert was prepared by:

- Dr. Viola Bensinger | +49 30.700.171.150 | viola.bensinger@gtlaw.com
- Carsten Kociok | +49 30.700.171.119 | carsten.kociok@gtlaw.com
- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Dr. Jannis Dietrich | +49 30.700.171.214 | jannis.dietrich@gtlaw.com