

Alert | Data, Privacy & Cybersecurity



November 2020

New Draft Standard Contractual Clauses for Cross-Border Transfers of Personal Data and Controller-Processor Relationships

*On 12 November 2020 the Commission of the European Union (EU) published two draft implementing decisions – one containing a **draft** new set of standard contractual clauses for transfers of personal data from the EU to third countries (the Cross-Border SCCs), and one containing a **draft** of new standard contractual clauses for certain clauses in controller-processor data processing agreements (DPAs) (pursuant to Article 28(7) GDPR). The Cross-Border SCCs were eagerly awaited by all stakeholders, even moreso after the Court of Justice of the European Union (CJEU) declared invalid the EU-U.S. Privacy Shield in its Schrems II ruling in July 2020. See **GT Alert** for further information.*

*Citizens and other stakeholders have until 10 December 2020 to provide **feedback** on the **draft Cross-Border SCCs** and on the **draft SCCs relating to DPAs**. After this date, the relevant committee will vote to accept or reject the draft decision.*

When can the new Cross-Border SCCs be used?

The published draft implementing decision on Cross-Border SCCs consists of two documents: (1) a main document with the decision itself and recitals explaining its application, aim, and scope; and (2) an Annex containing the actual clauses. The Annex follows a modular approach to cater to various transfer scenarios

and the complexity of today's processing activities. Parties to a transfer outside the EU may base such transfer on the general clauses and the respective module applicable to their processing situation at issue.

The new clauses can be used for the transfer of personal data:

- from controllers in the EU to controllers in a third country,
- from controllers in the EU to processors in a third country,
- from processors in the EU to a sub-processor in a third country,
- from controllers located in a third country subject to the GDPR to processors outside the territorial scope of application of the GDPR, and
- from processors located in a third country subject to the GDPR to sub-processors outside the territorial scope the GDPR.

This approach makes it possible for parties to tailor their obligations under the new SCCs to their corresponding role and responsibilities.

Why does it matter?

The current SCCs (old SCCs) are styled only to apply to transfers originating in the EU, not to extend to onward transfers. The *Schrems II* decision declaring invalid the EU-U.S. Privacy Shield Framework has caused a gap for a large number of data transfers from the EU to the U.S., and the onward transfers of such data. The uncertainty was further magnified by the CJEU when it required undefined "supplementary safeguards" for those transfers based on the old SCCs. However, precisely which "supplementary safeguards" might be necessary, or how to determine them, was not defined. Earlier in November, the European Data Protection Board offered some draft guidance on that issue (see [GT Alert](#)), and the proposed Cross-Border SCCs now offer some guidance as well.

What is new?

The proposed Cross-Border SCCs are the first of their kind issued under the GDPR and, as such, reflect the GDPR's requirements (whereas the old SCCs were drafted under the GDPR's predecessor, the Data Protection Directive). More importantly, their coverage is wider than that of the old SCCs – the new clauses cover additional processing and transfer situations and use a more flexible approach, for example, with respect to the number of parties able to join the contract.

The Cross-Border SCCs also provide for specific safeguards, in light of *Schrems II*. Such safeguards include explicit obligations on the data importer (i.e., the receiving party in the non-EEA "third country" of destination) in the case of governmental access requests to the data (e.g., reviewing the legality of such request and exhausting of all available remedies to challenge the request).

However, the new clauses do not relieve the parties to the processing arrangement from assessing and addressing the likely consequences of the third country's laws. In effect, the Cross-Border SCCs require the parties to perform a mini adequacy determination to evaluate whether the third country's laws would prevent the data importer from complying with the SCCs in practice.

Who is affected?

In the absence of an adequacy decision by the European Commission, according to the GDPR, a controller or processor may transfer personal data to a third country only if it has provided appropriate safeguards, and on the condition that enforceable rights and effective legal remedies for data subjects are available. The new clauses may provide such safeguards.

Therefore, once the Cross-Border SCCs are adopted, the controller or processor transferring the personal data to a third country (data exporter) and the data importer are free to conclude the Cross-Border SCCs to safeguard their processing. The new clauses may be included in a wider contract, and other clauses or additional safeguards may be added, provided they do not contradict the Cross-Border SCCs or prejudice the fundamental rights or freedoms of data subjects.

Apart from the original parties, additional controllers and processors may be allowed to accede to the new clauses as data exporters or importers at a later stage.

Are there any new obligations?

Yes, there are several new obligations. The Cross-Border SCCs:

- Require that data subjects be provided with a copy of the new clauses upon request and are informed, in particular, of any change of (a) purpose and (b) the identity of any third party to which the personal data will be disclosed.
- Provide that any onward transfer by the data importer to a recipient in another third country requires that either such recipient joins the SCCs or the data subject gives explicit, informed consent.
- Describe in more detail the liability between the parties and towards the data subjects and the indemnification obligations between the parties to the transfer.
- Impose certain obligations on processors and sub-processors as data importers comparable to the technical and organizational measures pursuant to Article 28 GDPR.
- Cover specific processing situations such as the merger of non-GDPR personal data with GDPR personal data by a data processor.
- Explicitly require a sub-processor to ensure compliance with the instructions of both the processor and the controller. This requirement may be challenging in practice when it comes to long processing chains with many links, including large cloud technology firms.

What are next steps?

As noted, citizens and other stakeholders can provide feedback on the draft until 10 December 2020. Once the relevant committee accepts the draft decision, there will be a one-year grace period from the date of entry into force of the decision introducing the Cross-Border SCCs. During this period, controllers and processors may continue to rely on the old SCCs as a cross-border data transfer basis for the performance of a contract concluded before that date; however, if material changes are made to such a contract, the data exporter can no longer rely on the old SCCs as its legal data transfer basis, and must have a new legal basis, for example, by entering into the Cross-Border SCCs. The same applies to any sub-contracting of processing operations covered by the contract to a sub-processor.

As there are only a few legal possibilities for companies to secure their data transfers, the Cross-Border SCCs have been eagerly awaited. In light of developments in the digital economy in recent years, including the widespread use of new and more complex processing operations often involving multiple data importers and exporters, coupled with long and complex processing chains and evolving business relationships, the Commission has provided a modernisation of the old SCCs to better reflect these realities.

Whether the Cross-Border SCCs can fulfil such purpose and provide a protective as well as practical solution for businesses in Europe (and elsewhere) remains to be seen.

What are the controller-processor SCCs?

The Commission separately proposed certain standard contractual clauses to be used between controllers and processors, as part of a DPA. These SCCs are the Commission's response to Article 28(7) GDPR, which allows the Commission to "lay down standard contractual clauses" for the contractual safeguards required by Article 28(3) and (4) GDPR when a data controller engages a data processor to carry out specific processing activities on its behalf.

For such data processing outsourcing relationships, the Commission has set forth these new SCCs for DPAs to standardize the data protection-related rights and obligations of the respective parties. It has also included detailed template annexes for the parties to use in describing the processing (with new fields for "records(s) of processing" and "place of storage and processing of data"); setting forth the technical and organizational safeguards (including bracketed prompts for descriptions of pseudonymization and encryption techniques, data recovery timeline requirements, events logging requirements, and user identification and authentication techniques); data controller instructions; specific restrictions concerning special categories of personal data; a list of sub-processors; and more.

As with the Cross-Border SCCs, the feedback consultation period for the controller-processor SCCs ends 10 December 2020. It is unclear at this time how widely adopted the controller-processor SCCs may become, given the variations in parties' bargaining power and the negotiations that generally take place in concluding data processing arrangements, but the Commission has set forth what purports to be a pre-approved guidepost for parties to potentially use as a baseline for such discussions.

Authors

This GT Alert was prepared by:

- [Viola Bensinger](#) | +49 30.700.171.150 | viola.bensinger@gtlaw.com
- [Gretchen A. Ramos](#) | +1 415.655.1319 | ramosg@gtlaw.com
- [Carsten Kociok](#) | +49 30.700.171.119 | carsten.kociok@gtlaw.com
- [Darren Abernethy](#) | +1 415.655.1261 | abernethyd@gtlaw.com
- [Johanna Hofmann](#) | +49 30.700.171.291 | johanna.hofmann@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany. ⁷ Houston. Las Vegas. London. ⁸ Los Angeles. Mexico City. ⁹ Miami. Milan. ¹⁰ Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul. ¹¹ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv. ¹² Tokyo. ¹³ Warsaw. ¹⁴ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ↯Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ⚡Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2020 Greenberg Traurig, LLP. All rights reserved.*