

Privacy, Security & Data Protection



JUNE 8, 2021 • NO. 3

New Standard Contractual Clauses for Cross-Border Transfer of EU Personal Data Released

The European Commission has published updated versions of the standard contractual clauses for international transfers of personal data from the European Union (“EU”). These new standard contractual clauses take into account both the Schrems II decision and the requirements of the EU General Data Protection Regulation (“GDPR”), and enable businesses to account for a variety of complex data transfers. The new standard contractual clauses will come into effect June 27, 2021, and businesses will have 18 months to update their data export/import arrangements.

On June 4, 2021, the European Commission released the final version of its [implementing decision](#) adopting new [standard contractual clauses](#) (“SCCs”) for use in connection with the transfer of personal data from the European Economic Area (“EEA”) to third parties outside the EEA. The new SCCs will replace the old versions of the SCCs, which were adopted many years ago under the EU Data Protection Directive, the precursor to the EU General Data Protection Regulation. The new SCCs are a culmination of efforts to update the SCCs to take into account the requirements of the GDPR and the July 2020 decision in [Schrems II](#) by the Court of Justice of the European Union (“CJEU”). In *Schrems II*, the CJEU invalidated the EU-U.S. Privacy Shield and held that SCCs could continue to be used for international data transfers, subject to parties ensuring that transferred data is afforded an adequate level of protection, which may require evaluation

and adoption of additional safeguards over and above those provided by the SCCs.

The new SCCs are effective June 27, 2021. Old versions of the SCCs will be repealed three months following publication of the implementing decision. After that time, the old SCCs may no longer be used for new data transfers. Contracts that already incorporate the old SCCs will continue to be valid for 18 months following publication of the implementing decision, provided the processing operations described in the contract remain unchanged. Accordingly, if a contract is negotiated and executed any time in the next three months, the parties may still choose to use the old version of the SCCs to cover international data transfers under that contract, though they will need to update those SCCs with the new SCCs before the expiration of the 18-month period.

HIGHLIGHTS OF NEW SCCS

- **Modular Terms:** In contrast to the prior set of SCCs that individually addressed a limited set of distinct transfer scenarios, the new SCCs take a modular approach that covers a broad range of transfer scenarios. This is intended to provide additional flexibility to account for the complexity of modern processing chains. The new SCCs may be used for (1) controller-to-controller transfers, (2) controller-to-processor transfers, (3) processor-to-processor transfers, and (4) processor-to-controller transfers. Controllers and processors will be required to select the module applicable to their role in relation to the data processing in question. Additional controllers and processors can accede to the SCCs if needed.
- **Schrems II Terms:** Consistent with the *Schrems II* decision and subsequent data protection authority [guidance](#), the new SCCs require parties to evaluate each transfer and document that an adequate level of protection is afforded to transferred personal data. Specifically, the SCCs require parties to assess (1) the details of the transfer, including the length of the processing chain, transmission channels, types of personal data, and purpose of processing, (2) the laws and practices of the destination country, including those requiring the disclosure of data to public authorities or authorizing access by public authorities, and (3) any relevant contractual, technical, or organizational safeguards to supplement the safeguards in the SCCs. The assessment must be provided to the competent supervisory authority upon request. Additionally, data importers must provide notification to the data exporter of legally binding requests from public authorities for the disclosure of transferred personal data and challenge the request if there are reasonable grounds to do so.
- **Onward Transfers:** The new SCCs prohibit onward transfers to additional recipients in third countries unless the onward transfer recipient agrees to be bound by the SCCs, or another specified exemption applies. Exemptions include transfers to recipients in such third countries that have been deemed to provide an adequate level of protection for personal data, entering into a binding agreement with the onward transfer recipient that ensures the same level of protection as the SCCs, or, if no other exemption applies, explicit consent from the data subject.
- **Use of Sub-Processors:** The new SCCs include form provisions for granting specific or general authorization for processors to engage sub-processors in the context of controller-to-processor and processor-to-processor transfers. Since the enactment of the GDPR in 2018, many companies operating as processors have developed form language for use in data processing agreements that are required between controllers and processors under Article 28 of the GDPR to account for such authorization. Commonly, these provisions account for specific operational limitations and efficiencies. For example, certain large-scale processors may post a list of sub-processors to a website but resist a requirement to create an operational mechanism to affirmatively provide the controller with advanced written notice of changes. Companies in the position of a processor that rely on SCCs will need to assess their processes for obtaining authorization for sub-processors in light of these new invariable form provisions.
- **Annexes:** The new SCCs include three annexes that must be completed. Annex I includes a list of the parties to the SCCs, a description of the personal data transfers, and the identity of the competent supervisory authority for each party to the SCCs. Annex II should describe the technical and organizational measures used to ensure an appropriate level of protection for the personal data. The clauses instruct that the security measures should be described in specific and not generic terms. Annex III should list sub-processors used by the processor processor if the processor has received limited specific authorization to engage sub-processors. Annex III does not apply in the case of general authorization.
- **Docking Clause:** The new SCCs allow for new parties (either as a data exporter or importer) to be added to already executed SCCs rather than requiring the SCCs to be re-executed. This will be especially helpful in the context of large-scale intra-group or extra-group data transfers.
- **Other Clauses:** The SCCs include a number of other general clauses that apply regardless of the type of transfer and role of the parties, including clauses relating to the redress mechanism available to data subjects, liability of the parties in the event of a breach of the SCCs, termination, choice of law, and jurisdiction.

NEXT STEPS

With the clock now ticking on phasing out old SCCs as a viable data transfer mechanism, businesses should:

- Inventory cross-border data transfers of European data in which they are involved, including the transfer mechanism used and identity and posture (*i.e.*, processor or controller) of parties involved in the transfer.
- Analyze the new SCCs to determine whether the new terms affect operational processes that have been put in place (*e.g.*, notification of sub-processing) or risk posture (*e.g.*, liability clauses) and determine whether process modifications or risk mitigation actions, such as reviewing insurance coverage, should be undertaken.
- To the extent not done already, implement and maintain processes for assessing the adequacy of protection afforded to transferred personal data consistent with the CJEU's *Schrems II* decision, data protection authority guidance, and the new SCCs. Create and maintain documentation of such assessments for each data transfer.
- For cross-border data transfers utilizing old SCCs, begin the process of replacing old SCCs with new SCCs. Determine if there are events within particular contractual relationships, such as renewal periods, that could be leveraged to replace terms with minimal disruption.
- For organizations involved in the transfer of personal data from the United Kingdom ("UK"), stay informed of data transfer guidance from the UK Information Commissioner's Office ("ICO"). The new SCCs are not automatically approved for use in connection with UK personal data transfers. However, the ICO is expected to adopt similar clauses in the relatively near future.

For additional information, please contact:

Sharon R. Klein

949.812.6010 | sharon.klein@blankrome.com

Jennifer J. Daniels

412.932.2754 | daniels@blankrome.com

Alex C. Nisenbaum

949.812.6011 | alex.nisenbaum@blankrome.com

Karen H. Shin

949.812.6012 | karen.shin@blankrome.com