CLIENT ALERTS & INSIGHTS

Revised Approach to Standard Contractual Clauses Creates Key Deadlines and Offers Long-Awaited Answers

JUNE 15, 2021

Authors: Ryan T. Sulkin, Michael D. Stovsky

The European Commission's long-awaited updates to the Standard Contractual Clauses ("SCCs") have arrived. Data protection lawyers globally have eagerly anticipated these changes, which are necessary to address a legal landscape re-made by the GDPR and, more recently, the Schrems II decision.

What are the Key Deadlines?

The new SCCs will become effective twenty (20) days following their publication in the Official Journal of the European Union (placing the anticipated effective date in the end of June or early July timeframe). The new SCCs are eligible for use immediately after their effective date. With respect to the old SCCs, there are two (2) key dates to keep in mind.

- The old SCCs can only be newly signed for a period of three (3) months after the new SCCs come into effect. Thereafter, only the new SCCs can be newly signed.

- Versions of the old SCCs signed prior to the cut-off date noted above are considered "grandfathered in" and are therefore deemed valid for an additional period of (15) months following the cut-off date provided that:

    - The processing described under the old SCCs has not changed; and

    - Reliance the old SCCs ensures that the transfer of personal data is subject to appropriate safeguards (which means in practice that the risk assessment required by *Schrems II* will need to be completed).

Bottom line, all old SCCs will need to be replaced within approximately 18 months.

What is the purpose of the SCCs?

Taking a step back, the historical purpose of the SCCs (as carried forward under the GDPR), was to allow for the transfers of personal data from geographic locations within the European Economia Area (EEA) to geographic locations outside of the EEA deemed not to have adequate data protection law. The United States is one of many countries deemed to have inadequate data protection law by the EU. Use of SCCs has grown significantly in recent years as a result of the instability of the EU-US Privacy Shield program and its predecessor, the EU-US Safe Harbor program.

How have the SCCs changed?

The new SCCs come in two (2) different sets.

The first set of SCCs addresses the traditional paradigm, transfers of personal data from geographic locations within the EEA to geographic location outside of the EEA. However, unlike the old SCCs which only offered controller to controller and controller to processor versions, this first set of new SCCs offers two additional options (four options in total) as follows: (i) controller to controller; (ii) controller to processor; (iii) processor to processor; and (iv) processor to controller, covering data sharing paradigms that the old SCCs struggled to address with clarity. The second set of new SCCs, which did not exist in a prior form, covers the engagement of data processors in the EEA when a cross-border data transfer outside of the EEA is not involved and satisfies the requirements for engaging processors under Article 28 of the GDPR.

What about the *Schrems II* decision?

The first set of new SCCs contain contractual provisions designed to address the concerns raised by the *Schrems II* decision, including specific obligations when there is a government request for personal data in a non-EEA destination country. For example, the data importer is required to challenge government access requests if there are reasonable grounds for doing so and pursue possibilities of appeal where reasonable. The data importer must document its legal assessments in this respect and make them available to the data exporter and the competent supervisory authority upon request. The new SCCs also require the signing entities to conduct and document a data transfer impact assessment and make it available to the competent supervisory authority upon request. When undertaking their data transfer impact assessment, the parties may consider "relevant and documented practical experience with prior instances of request for disclosure from public authorities, or the absence of such requests". In addition, further guidance from EU regulators may require additional contractual or operational protections beyond language currently in the new SCCs. Accordingly, this is an area that must be monitored closely.

Additional Interesting Details

- The new SCCs permit a data exporter to be established outside the EU, aligning with the extra-territorial reach of the GDPR.

- The new SCCs also enable multiple parties to enter into the SCCs, aligning with how many organizations currently address intra-group data transfers (essentially, versions of the SCCs entered into by relevant company affiliates to address EEA to non-EEA personal data transfers).

- The new SCCs state: "each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses." As a result, it remains an open question as to whether the SCCs will allow one party to limit their liability to the other party by adding bolt on language to the SCCs, which is currently a common practice.

- Annex II of the new SCCs requires more specific detail with respect security measures in place and offers more specific suggestions for these measures.

- Currently, the new SCCs are not required for transfers of personal data from within the UK to outside of the UK; however, a similar SCC construct will likely be required by the UK in the future. It is also currently undecided as to whether the European Commission will require SCCs for personal

data transfers from the EEA to the UK (or whether the UK will be deemed “adequate” such that SCCs are not required).

Takeaways

Now that the new SCCs are a known commodity, it is time for organizations to design and begin implementation of a comprehensive strategy for replacement of existing SCCs, both with third parties and as between their own affiliates in the intra-group personal data transfer context. In addition, enhanced procedural and documentation requirements within the new SCCs mean that signing the SCCs will be much more than an exercise on paper, making the need to prepare early all that more important. The Data Protection team at Benesch is available to answer any questions that you may have and support your organization with its transition to the new SCCs.

For more information, please contact a member of Benesch's Data Protection Team.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Michael D. Stovsky at mstovsky@beneschlaw.com or 216.363.4626.