WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

European Commission Adopts New Standard Contractual Clauses

June 14, 2021

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Richard M. Borden | Henrietta de Salis
Marilena Hyeraci* | Stefan Ducich

On June 4, 2021, the European Commission ("Commission") adopted a new set of Standard Contractual Clauses ("SCCs") for transfers of personal information from within the European Union ("EU")/European Economic Area ("EEA") to third countries under the General Data Protection Regulation ("GDPR"). This follows the publication in November 2020 of draft SCCs, and a subsequent consultation period.[1] The new SCCs provide some clarity for cross-border data transfers, by replacing the current clauses – which were adopted by the Commission under privacy laws that pre-date GDPR – and attempting to address the legal uncertainties regarding transfers of personal data to third countries arising out of the EU Court of Justice's decision in *Schrems II* (invalidating the EU-U.S. Privacy Shield program). However, questions remain.

For many U.S.-based companies doing business in the EU, or EU companies doing business with U.S.-based partners, the SCCs have become a key component of their efforts to legitimize the transfer of personal data in compliance with GDPR. Such companies will need to begin the process of updating and amending existing agreements to incorporate the new SCCs and, where appropriate, implement new (and potentially significant) operational and legal measures, including ad hoc trainings and the development and maintenance of appropriate documentation, to achieve compliance.

* Marilena Hyeraci is an associate at Studio Legale Delfino e Associati.

1 Draft Commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, here.

Background

GDPR provides a number of legal bases for transfers of personal data from within the EU/EEA to third countries,[2] including, among other mechanisms, the existing SCCs. The existing SCCs are an imperfect tool, as they do not align with the current legal (or operational) landscape in which data transfers and data processing occurs. The new SCCs may be adopted without modification, or may be modified provided any changes or additional clauses do not directly or indirectly contradict the SCCs or reduce protections for data subjects.

Moving Forward

The new SCCs incorporate important developments as part of the Commission's effort to align the clauses with EU law and current market practices. Companies involved on an international basis in the processing of personal data from within the EEA will need to adopt the new SCCs in due course, and should begin planning for that now. Below are a few key aspects of the new SCCs to consider.

Timing and Transition Period

The new SCCs come into force on June 27, 2021; but there are two transitional arrangements, which give companies time to enter into the new SCCs.

First, regarding already executed contracts using the existing SCCs, companies have eighteen months (**until December 27, 2022**) to update their SCCs, provided that processing operations remain unchanged during that period and transferred personal data is subject to proper safeguards.

Second, for new contractual arrangements, companies may use the existing SCCs **until September 26, 2021**. Such contracts will be deemed to provide appropriate safeguards until December 27, 2022, subject to the same restrictions noted above. (Alternatively, such new arrangements could use the new SCCs). Beginning September 27, 2021, all new contracts for the processing of personal data must use the new SCCs.

Modular approach

As previewed in the November 2020 draft, the new SCCs adopt a modular approach to address multiple transfer scenarios (i.e., controller-to-controller, controller-to-processor, processor-to-(sub-)processor, and processor-to-controller). The data exporter and data importer select the module appropriate to the nature of the export, which tailors their obligations and defines the purpose limitations of the transfer. The parties thus blend general SCC clauses with specific modules (and applicable annexes); ad hoc sections and restrictions are provided in connection with sensitive data.

[2] Third countries do not include countries such as Switzerland, where the EU has granted an adequacy decision, such as Switzerland.

The new SCCs require greater detail regarding the parties, the categories of data subjects, and personal data involved in the transfer – including the frequency of the transfer, and in some cases, identifying the competent supervisory authority. Moreover, depending on the specific module applied, the importer(s) must describe the specific technical and organizational measures in place to ensure the security of the transferred data.

This modular approach better addresses the more complex processing arrangements involving a chain of processors.

Risk Assessments & Schrems II

The new SCCs expressly aim to address the concerns raised by *Schrems II*, in part by requiring data exporters and data importers to assess risks posed by the laws of third country destinations, and to account for such risks by providing specific safeguards – in particular with respect to dealing with binding requests from public authorities. Parties must assess the local laws and practices of the third country destination, and warrant that they have no reason to believe such laws or practices would prevent the data importer from fulfilling its obligations under the SCCs.

The risk assessment required under the new SCCs is meant to be collaborative, and the parties may conclude there is no impediment to compliance with the SCCs based upon considerations of "relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe."[3]

To the extent the parties determine that such "relevant and objective" elements are deemed sufficient,[4] this determination should be documented. Additionally, if the data importer has reason to believe it will not be able to comply with the SCCs, or upon receipt of a "legally binding request"[5] from a competent public authority for access to transferred personal data, the data importer must inform the data exporter. If the parties cannot identify appropriate compensating safeguards, the parties must suspend such transfers.

Ensuring Security & Personal Data Breach Notifications

The parties to the SCCs must implement and maintain appropriate technical and organizational data security measures, including with respect to protecting against a personal data breach. These security requirements are more detailed than those in the current SCCs, and require a higher standard for both the data exporter (which must ensure the implementation of appropriate security measures during transmission) and the data importer (which must regularly confirm the safeguards' efficacy and ensure appropriate confidentiality commitments are in place). Moreover, the new SCCs

3 Annex to the Commission implementing decision (EU) 2021/914 of 4 June 202 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council clause 14, n. 12.

4 *Id*.

5 *Id*. at clause 15.1(a)(i).

introduce a duty on the data importer, which may be a data processor under GDPR, to notify data exporters, the relevant supervisory authority, and in certain instances, affected individuals in the event of a personal data breach (whereas GDPR requires the data processor to notify only the data controller).

Liability & Redress

Under the new SCCs, data subjects are deemed to be third party beneficiaries. This allows data subjects to invoke and enforce several provisions of the SCCs, without prejudice to data subjects' rights under GDPR. Complaints may be submitted to the designated member state supervisory authority (per new SCC Annex 1) and the courts of that member state are competent to resolve disputes arising under the SCCs. Additionally, the SCCs provide for rules on allocating liability (including with respect to data subjects).

Scope

The new SCCs correct for the territorial misalignment in the prior clauses. The existing SCCs only provide for a "data exporter," established in the EU/EEA. However, a company that is established in a third country, but which provides goods or services in the EU/EEA (and thereby collects personal data from individuals within the EU/EEA), is subject to GDPR. The new SCCs may be applied where personal data is transferred by a controller or processor subject to GDPR – irrespective of the data exporter's location – to a controller or (sub-)processor whose processing of the data is not subject to GDPR (the data importer). The law governing the SCCs must be that of an EU member state.

The new SCCs also allow for multiple parties to join as data exporters or data importers, and allow parties to later join or accede to the clauses via the "docking clause."[6] This is meant to promote flexibility and efficiency in ensuring the protection of personal data. This may be particularly useful in the context of mergers and acquisitions or for intra-group transfers where new group companies may be created over time.

Practical Outcomes

The new SCCs will create substantive and procedural requirements for both data exporters and data importers, including new and specific obligations regarding risk assessments, technical and organizational security requirements, and other procedures. For many companies, this will likely necessitate the development of internal procedures, as well as collaborative efforts between the parties establishing the data exporter-data importer relationship (i.e., the risk assessment is a fact-based, transaction-specific process that may increase diligence in M&A deals, or require the development of technical, legal, and/or operational expertise to conclude such contracts).

[6] *Id*. at clause 7.

Moreover, the allocation of liability will require focused analysis by the parties to properly address risk. Data importers may seek indemnification to address changes in the allocation of liability that currently exist under contract. To the extent that terms of commercial liability conflict with the new SCCs' liability provisions (or undermine the rights of data subjects), such terms may invalidate the adequacy or legal basis of the SCCs as a transfer mechanism.

The new SCCs mirror the GDPR's data processing principles, and impose these requirements on data importers. These are reflected in enumerated obligations for both parties around purpose limitations, transparency, data minimization, accuracy, and storage limitations, which imply requirements to review, for instance, the information notices and consents of data subjects, data retention policies, IT and privacy policies, security measures, and the provision of more detailed instructions to processors and sub-processors.

Importantly, the SCCs also import "accountability" in the form of documentation and compliance provisions throughout the modules. As such, the parties must maintain appropriate and sufficient documentation, such that compliance may be "demonstrated."

What's next?

While the new SCCs provide much needed clarity around transfers of personal data to third countries, several questions remain open.

- *Will the new SCCs provide sufficiently robust safeguards to support cross-border transfers?*

Unclear. The risk assessment framework may address the concerns of the *Schrems II* decision, but we'll likely have to wait for any court decision for a final answer. Certainly, the consideration of "relevant and documented practical experience" concerning prior requests – *or lack thereof* – is a nod towards the practical reality of transfers to the United States; however, EU courts and regulators may still effectively eliminate this avenue by deeming US law insufficiently protective of personal data.

- *How will the UK deal with the SCCs?*

During the "Brexit" transition period, the UK Information Commissioner's Office ("the ICO") advised that the existing SCCs would continue to be valid until the adoption by the UK of its own SCCs. The ICO has said that it is working on new UK SCCs and we expect the ICO to publish these for consultation this summer. It is likely that new UK SCCs will be similar to the Commission's new SCCs because (a) the ICO will also want to account for *Schrems II*, and (b) any adequacy decision granted by the EU in favor of the UK (expected this month) will be dependent on the UK maintaining the same standards of data protection as under GDPR.

- *How will parties address the substantive requirements of the new SCCs and GDPR?*

The new SCCs will require careful consideration, particularly on the part of companies operating outside the EU/EEA that are subject to GDPR as data exporters or as (sub-) processor data importers.

The European Data Protection Board is expected to release the final version of its Recommendations 01/2020 and 02/2020 on *Schrems II* by mid-June, which may prove useful regarding the due diligence and risk assessment relating to local laws affecting SCC compliance.

The new SCCs require additional layers of scrutiny – regarding the structure and details of the personal data transfer, risks arising from the transfer, allocating liability, inclusion of audit rights, the impact of data subjects as third party beneficiaries, and more. This will be a significant undertaking; despite the transitional period of eighteen months, the iterative process of contract negotiation and regulatory interpretation will take time. Companies should begin this process as soon as possible to ensure they are capable of meeting their obligations under the new SCCs by December 2022.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Henrietta de Salis
+44 20 3580 4710
hdesalis@willkie.com

Marilena Hyeraci
+39 02 76363 1
mhyeraci@delfinowillkie.com

Stefan Ducich
+1 202 303 1168
sducich@willkie.com