Articles + Publications | July 22, 2021

New Standard Contractual Clauses Supply Opportunities and Obligations for Organizations Transferring Personal Data Out of the EU

WRITTEN BY

Alison A. Grounds | Angelo A. Stio, III | Molly S. DiRago | Jim Calvert | Edgar Vargas | Brett A. Dorman

On June 4, the European Commission (Commission) adopted new standard contractual clauses (SCCs) for the transfer of personal data to third countries. SCCs have long been an important tool for EU data transfers, as one of only a handful of mechanisms available to legitimize personal data transfers made to countries outside the European Union (EU). This importance increased in July 2020 when the EU Court of Justice (CJEU) issued its decision in *Data Protection Commission v. Facebook Ireland, Max Schrems (Schrems II),* which invalidated the EU-U.S. Privacy Shield, another oft-used mechanism to effectuate cross-border transfers of EU data to the U.S. Critically, in *Schrems II*, the CJEU upheld the validity of SCCs, but found that data transferors must verify the adequacy of protections available in jurisdictions to which data is transferred on a case-by-case basis. These new SCCs, replacing the older pre-GDPR iterations and arriving in the wake of *Schrems II*, include several improvements that should help data exporters ensure adequate protections and innovations, while allowing for more flexible and streamlined drafting.

Drafting Features

While the old SCCs were limited to two separate templates for controller-to-controller and controller-to-processor transfers, the new SCCs feature interchangeable “modules” to create clauses for the variety of data transfers prevalent today.

Such new modules include:

- From a controller to another controller;
- From a controller to a processor;
- From a processor to a processor; and
- From a processor to its appointing controller.

The new SCCs also include “docking clauses” for multiparty use that allow for change over time. Additionally, the new SCCs contemplate that data exporters may be located outside the EU, an important innovation in light of the GDPR’s extraterritorial reach.

These new features alleviate difficulties that often arose in multistep transfers under the prior SCCs, especially where an EU-based data controller transferred to a U.S.-based data processor that thereafter transferred to a sub-processor. Under the prior SCCs, which did not allow for non-EU data exporters or for processor-to-processor transfers, the controller might have executed separate, parallel SCCs with both processors — an imperfect and inefficient solution. The new SCCs allow this model to be covered in a single agreement joined by all three parties, with modules clearly laying out responsibilities for both the controller-to-processor (EU-to-U.S.) and processor-to-processor (U.S.-to-U.S.) transfers.

An additional drafting benefit is that the new SCC modules for controller-to-processor and processor-to-processor transfers no longer require a separate data processing agreement be in place. This feature should streamline the drafting process by alleviating the potential for inconsistencies that existed in the old framework.

Increased Protections

The new SCCs add significant requirements in line with the GDPR and the *Schrems II* decision by increasing the level of data protection for covered transfers. These enhancements include additional importer transparency, accountability, and recordkeeping requirements, as well as data subject rights to access, delete, and object to processing for direct marketing. Under the new SCCs, data importers must challenge government access requests if there are reasonable grounds for doing so. Also, importers must report such requests transparently and notify the exporter if they cannot comply with the SCCs in light of such requests, at which point the exporter may suspend or terminate the SCCs if necessary.

Risk-Based Approach

Clause 14 of the new SCCs requires that the parties warrant that they have no reason to believe that the laws and practices of the data importer's country will interfere with the data importer's ability to fulfill its obligations. Accordingly, the parties must make a thorough assessment of the potential impact of such laws and practices, document the assessment, and make it available to supervisory authorities on request. Crucially, the Commission included in a footnote that this evaluation "may include relevant and documented *practical experience* with prior instances of requests for disclosure from public authorities, *or the absence of such requests*." (emphasis added). This allows parties to base their risk assessments not only on the government's *authority* to seek data, but also on their good faith assessment of the actual likelihood of government access to the data in question.

The new clauses provide factors that the data exporter (based on input from the importer) must consider when performing a transfer impact assessment:

- The law and practice in the third country;
- The purpose of the processing;
- The nature of the data transferred;
- The length of processing chain;

- The number of actors involved;
- The transmission channels used;
- The type of recipient and details of the transfers;
- The format of the transferred data;
- The relevant economic sector in which the transfers occur; and
- The storage location of the data transferred.

Implementation Timeline

Parties utilizing SCCs have two critical timelines to plan toward. First, for new data transfers needing legitimization via SCCs, parties may use the old SCCs up until September 27, 2021 (three months after the effective date of the new SCCs). Second, old SCCs executed before September 27, 2021 will be valid for another 15 months, until December 27, 2022.

This advisory summarizes some important aspects of the new SCCs, including features that should benefit data transferors and ease the drafting process. At the same time, the new SCCs are complex and will require careful evaluation of existing and new data transfer arrangements to ensure the adequacy of protections and compliance with the SCCs themselves. Accordingly, all organizations relying on SCCs should develop a plan to replace existing SCCs and ensure compliance with requirements in the new SCCs as soon as practicable.

United Kingdom Considerations

Importantly, post-Brexit, while the United Kingdom (U.K.) adopted the GDPR in nearly identical form, the new EU SCCs cannot be used for U.K.-specific, cross-border data transfers. The U.K.'s Information Commissioner's Office (ICO) is working on its own set of standard contractual clauses that it plans to release, and it has published for consultation the European Data Protection Board's "recommendations on measures that supplement transfer tools." However, until the ICO releases its new SCCs, the U.K. has created a U.K. version of the previous SCCs (with guidance), which should be used for the time being (but only for U.K. cross-border data transfers).

We will continue to follow the U.K.'s development of its SCCs and provide future alerts as new materials are released.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber