Out with the Old, In with the New SCCs

Alysa Z. Hutnik, Aaron J. Burstein, Alexander I. Schneider

September 29, 2021

As of September 27, 2021, the European Commission requires controllers and processors to rely on the recently updated Standard Contractual Clauses (SCCs) for any **new** contracts governing personal data transfers from the EEA. (Existing contracts can continue to use old SCCs until December 27, 2022.) This post provides an overview of what's in the new SCCs and how they compare to the old clauses they replace.

The Need for New Standard Clauses. Like the old SCCs, the new SCCs are model data transfer provisions designed to provide an "adequate" level of data protection in countries that have not received an adequacy determination ("third countries").

A lot has changed, however, since the European Commission developed the old SCCs; and the SCCs were due for an update. The old SCCs were based on the GDPR's predecessor, the Data Protection Directive 95/46/EC, and only addressed controller-to-controller transfers (issued in 2001) and controller-to-processor transfers (2010), respectively. The previous SCCs did not cover processor-to-processor transfers or processor-to-controller transfers, and gave limited choices for governing law and venue to resolve disputes, among other limitations.

In the intervening years, data transfers have increased in complexity and volume. The GDPR imposes its more comprehensive obligations on controllers and processors. And the *Schrems II* decision, which invalidated the EU-US Privacy Shield, requires analysis of surveillance practices and other conditions in third countries such as the United States.

Key Changes. The new SCCs apply to a more complete range of data relationships and are divided into four different modules:

- (Module 1) controller to controller;
- (Module 2) controller to processor;
- (Module 3) processor to sub-processor; and,
- (Module 4) processor to controller.

These modules are covered by a single draft of the SCCs (unlike the old SCCs, which were issued in two separate decisions, which were a source of much confusion).

The new SCCs more closely mirror the GDPR's requirements and address important issues raised in the *Schrems II* ruling. *Schrems II* focused on the potential harm to EEA data subjects whose information was transferred outside of the EEA and could be accessed by third-country authorities in bulk and without sufficient safeguards. The European Commission included several contractual terms

in the new SCCs to address these concerns, such as:

- **Clause 14:** Parties provide contractual warranties regarding protections for personal data in cases of access by authorities;
- **Clause 15:** Data importer agrees to further obligations in cases of a request for disclosure by authorities, including to notify the data exporter, review the legality of the request for disclosure, appeal if the request is unlawful under international law, and provide the minimum information possible to a request;
- **Annex II:** SCCs provide an opportunity to list all supplemental technical and organizational measures used to protect personal data.

What About the UK? It is important to note—since the UK recently left the EU and the transition period for its withdrawal expired at the end of 2020—the SCCs do not automatically apply to the UK GDPR. However, the *Schrems II* decision does apply to UK law because it was handed down in 2020 during the Brexit transition period. The UK Information Commissioner's Office (ICO) is expected to come out with guidance in the coming months for revisions to the SCCs under the UK GDPR that incorporate the *Schrems II* provisions.

Practical Impact. Any contracts that were finalized prior to September 27, 2021 can continue to rely on the old SCCs until December 27, 2022 as long as the data processing obligations remain unchanged.

It would be worthwhile for data importers to take stock of their data collection practices and review their responsibilities under the new SCCs. This is a good time for companies to determine whether their DPAs have terms that are inconsistent with the new SCCs and, if they do, to resolve those inconsistencies. For companies that have global DPAs, an SCC-driven review presents a good opportunity to update the DPA to account for new contract requirements from the CPRA, VCDPA, and ColoPA. For example, the CPRA requires third party contracts to include provisions limiting personal information sales to specified purposes. Both VCDPA and ColoPA require controllers to have contracts with specific instructions on how the processors must process data such as the type and duration of processing.