wiley

NEWSLETTER

The European Commission Releases Updated Standard Contractual Clauses for International Data Transfers

June 2021

Privacy In Focus®

On June 4, 2021, the European Commission (EC) released the long-awaited updated Standard Contractual Clauses (SCCs) for data transfers outside of the European Economic Area (EEA). The updated SCCs not only bring the SCCs in-line with the requirements of the GDPR, but they also address the additional data transfer safeguards raised by the *Schrems II* decision. This article provides a high-level overview of key changes to the SCCs and highlights important timing considerations for companies that currently rely or plan to rely upon on SCCs as a cross-border data transfer mechanism.

SCCs, in general, create a contractual obligation between parties to safeguard data transferred outside of the EU that is "essentially equivalent" to the protection requirements of the GDPR, and – subject to certain additional considerations – are recognized as a valid data transfer mechanism. SCCs took on increased importance in the wake of the *Schrems II* decision that invalidated the U.S.-EU Privacy Shield, another data transfer mechanism relied upon by many U.S.-based businesses, as discussed here.

Key Changes to SCCs for Cross-Border Personal Data Transfers

The updated SCCs are structured with a **modular approach** to address a variety of data transfer scenarios, including (i) Controller to Processor, (ii) Controller to Controller, (iii) Processor to Processor, and (iv) Processor to Controller. The provisions of each module include the required disclosures and commitments for each party. The previous

Authors

Joan Stewart
Of Counsel
202.719.7438
jstewart@wiley.law

Practice Areas

GDPR and Global Privacy
Privacy, Cyber & Data Governance

SCCs were more restrictive, addressing only Controller to Controller or Controller to Processor relationships. This update is welcome as it provides flexibility to address the variety of data transfer situations encountered in most business relationships.

The updated SCCs can be incorporated into a commercial contract and, unlike the current SCCs, **additional clauses may be added**, provided they do not undermine the validity of the SCCs (or compromise the rights of individuals).

A **docking clause** is included which allows entities that are not the original parties to the SCCs to assent to the SCCs without entering into a separate contract. As a practical matter, this clause will be helpful if more entities are added to the data transfer chain.

The parties to the updated SCCs may also elect to authorize the use of **sub-processors** either by specific prior authorization of listed sub-processors or by a general written agreement to the use of sub-processors.

The new SCCs permit the **onward transfer** of personal data by the data importer only when certain criteria are met. These include where the new recipient accedes to the SCCs (See docking clause above), when the receiving country has received an adequacy decision, or when certain conditions have been met (which will differ by module), such as consent of the data subject.

Cross-border data transfer safeguards in response to the ***Schrems II* decision** are incorporated into Clauses 2 and 3 of the SCCs.

- Clause 2 requires that the parties warrant "that they have no reason to believe the laws in the third country of destination applicable to the processing of personal data by the importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses."
- To be able to make this representation, the parties must assess the specific circumstances of the transfer, the laws of the destination country, and any safeguards that have been implemented in addition to those required by the SCCs (e.g., encryption).
- Documentation of the assessment must be retained and provided to the supervisory authority upon request.
- If the data importer can no longer comply with the SCCs, it must notify the data exporter.
- Should the data importer receive a binding request from a public authority, Clause 3 requires the data importer to take specific and extensive requests to avoid disclosing data to that authority. Should the importer be compelled to disclose data, they should disclose the minimum required data.

Timing and Next Steps for the New SCCs

The SCCs will become effective 20 days after publication in the Official Journal of the EU and the old SCCs will be repealed three months after the updated SCCs take effect.

Once the SCCs are repealed, businesses must use the new SCCs in any new contracts. Businesses will have an additional 15 months after the old SCCs are repealed to transition existing contracts to the updated SCCs.

We encourage businesses to immediately focus on the process to roll out the updated SCCs, as the transition process may be complicated. Businesses will need to evaluate their contracts involving data transfers from the EU to determine which SCC module best fits that contractual relationship. Likewise, the business will have to assess and document its compliance with the additional *Schrems II* obligations required by the new SCCs. Finally, businesses will need to revise existing contracts to include the SCCs.

Our team has helped entities of all sizes from various sectors parse through complicated GDPR issues – from determining whether the GDPR applies to developing compliance programs. If your organization has questions about the GDPR or the potential impact of the new SCCs on your business, do not hesitate to reach out.