STINSON

News & Insights

EU Authority Publishes New Standard Contractual Clauses

Alert
06.15.2021

By David Jennings and Steve Cosentino

Since the implementation of the EU's General Data Protection Regulation (GDPR), the European Commission's (EC) approved Standard Contractual Clauses (SCC) have been vital to the transfer of personal data to third countries outside of the EU, particularly the United States, which is deemed by the EU to lack adequate protection for personal information. On June 4, 2021, the EC adopted long-awaited and updated sets of "new SCCs"—one for use between data controllers and those that process that data, and the other for the transfer of personal data to third countries, such as the U.S. Since the European Union's top court (Court of Justice of the European Union) invalidated the EU-US Privacy Shield Framework in its July 16, 2020 *Schrems II* decision, those responsible for compliance with personal data privacy practices in the United States and the European Economic Area have been waiting for the EC to adopt these new SCCs.

Use of SCCs by U.S. businesses, both large and small is ubiquitous. The current version of the SCCs was approved by the EC in 2010. SCCs typically form part of data protection agreements with vendors and service providers and are intended to comply with the requirements of the GDPR. With the EU-US Privacy Shield invalidated in the EU, U.S. based companies that require the movement of personal data back and forth between the EU and the U.S. will more heavily rely on the new SCCs. The *Schrems II* decision left some ambiguity as to whether the SCCs were valid as a transfer mechanism so adoption of these new SCCs is a welcome development on this side of the pond.

Expanded Scope

The new SCCs retain a modular approach. They include new modules that cover an expanded scope of data transfer modes.

The prior version of the SCCs could only be used by data exporters in the EU that were data controllers—meaning the entities that determine the methods and means of processing personal information. That left U.S. privacy compliance personnel scratching their heads as to how to handle situations where a processor in the EU transfers personal data to a sub-processor outside the EU. There were also no approved clauses for use by data exporters that are subject to the GDPR but are not established in the EU.

The new clauses address these gaps, with content for use in controller-to-controller, controller-to-processor, processor-to-sub-processor and processor-to-controller situations. They also expressly state the new SCCs can be used by parties that are not established in the EU. For example, a U.S. company could retain the services of an EU-based call center to respond to customer queries arising from sales made in the EU. The new SCCs form for a processor-controller transfer would allow that call center to share customer records with its U.S.-based client. That call center could now also sub-contract its work to an overflow call center outside the EU, using the processor-processor form.

Multipartite Clauses and Docking

The new SCCs now expressly allow for multiple data exporting parties to contract, and for new parties beyond the initial signatories to be added to them over time (the so-called "docking clause"). The prior SCCs were drafted as two-party agreements, capturing the relationship between two parties as they existed at a static point in time. Despite it being a relatively simple drafting modification to the prior SCCs to allow for extra parties (whether at the point of contracting or added over time), it was uncertain if this was permitted. The docking clause additions now make clear and make it reasonably easy to add parties to existing agreements.

Additional Obligations and Transfer Impact Assessments

The new SCCs incorporate additional obligations that trace back to issues raised in the *Schrems II* decision. One of these key additions is that data exporters are now obligated to conduct and document a transfer impact assessment (TIA)—assessing the sufficiency of non-EU country protections on a case-by-case basis prior to transferring data from the EU to the non-EU country. This TIA must be made available to the competent EU supervisory authority on request. The SCCs set out the factors that the data exporter must consider in a TIA. The new SCCs provide a welcome answer to the biggest question that companies, regulators and policymakers faced in the wake of the *Schrems II* decision. Namely, whether or not TIAs should be not risk-based or whether companies should be allowed to rely on "subjective factors," such as the likelihood of government access requests (e.g., as allowed under FISA §702) based on past experience.

Specifically, the implementing decision for the SCCs recites that a risk-based analysis may be utilized, stating:

> ...As regards the impact of such [local U.S. laws] and practices on compliance with the standard contractual clauses, different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by

> independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer.

Time will tell whether it proves true, but many privacy professionals in the U.S. are hoping that by permitting this experience and risk-based analysis as part of a transfer impact assessment, the EC has smoothed the way for most U.S. data importers to avoid implementing additional (and potentially cumbersome) measures beyond the express requirements of the SCCs in order to comply with the GDPR. Such measures, are commonly referred to as, "supplementary measures," and include technical measures, such as data encryption, and additional organizational and structural processing measures.

What does this mean for your business?

The EC implementing decision becomes effective on June 27, 2021. The new SCCs come into effect on September 27, 2021. From that September date, the EC has provided for a 15-month transition period. Thus, all existing contracts entered into prior to September 27, 2021 will, unless amended or changed after that date, will be valid for the duration of the transition period, which expires on December 27, 2022. The new SCCs must be used for any new contract entered into after September 27, 2021, and for any existing contract that was entered into prior to September 27, 2021, but to which an amendment is made during the 15-month transition period. By December 27, 2022, all contracts utilizing SCCs, must incorporate the new SCCs.

During this transition period, businesses should take an inventory of all existing SCCs and develop a plan to obtain replacement SCCs by December 27, 2022. Implementing the new clauses will take significant effort —both because of the requirements associated with documenting transfer impact assessments, and because of the requirements to provide enhanced information to data subjects and to flow-down the same terms to third parties/sub-processors if there are onward transfers.

Businesses should also be careful to determine where ill-fitting versions of the prior SCCs should be replaced with more appropriate versions of the new SCCs. Plan for some significant time to get the new SCCs replaced because compliance efforts tend to lag behind getting current transactions complete. The new SCCs should also be included in data protection agreements going forward.

There is much more included in the new SCCs than can be described here, some of which may be viewed positively by U.S. based businesses and some of which may be burdensome. Over the coming weeks and months, privacy professionals will continue to evaluate the new SCCs and we will work to keep you up to date on what works well, and what doesn't, as this implementation effort gets underway.

CONTACTS

Stephen J. Cosentino, CIPP

David B. Jennings, CIPP/E

EU Authority Publishes New Standard Contractual Clauses

RELATED CAPABILITIES

Cybersecurity & Data Privacy

International

Telecommunications