COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2022
Deconstruct 'contract chaos' to comply with EU data transfer rules

By Zachary Foreman

Zachary Foreman (zachary.foreman@knowable.com) is Offerings Lead for Knowable in Mainz, Rhineland-Palatinate, Germany.


Zachary Foreman

In June 2021, shortly after the third birthday of the General Data Protection Regulation (GDPR) and on the heels of the Schrems II decision, the European Commission released new editions of the standard contractual clauses (SCCs). With them has come another headache for privacy, legal, and compliance professionals: a complex project of updating executed contracts in order to maintain compliance with the latest developments in the international data transfer regulatory regime.

Amending contracts at scale to reflect the latest SCC changes requires the focused application of people, process, and technology. But the real challenge—maintaining contract compliance in a shifting regulatory environment—requires systematically monitoring your organization's contractual provisions in order to execute projects, demonstrate compliance, and measure risk across the organization.

How SCCs regulate data transfers

SCCs are a vital tool in the modern data protection compliance toolkit, but what are they, and how are they used? SCCs are the most important way that the European Union (EU) ensures that its residents' data rights remain protected even when the data itself is transferred to another country with other, less stringent regulations. The European Commission can't require other countries to enforce its rules overseas, but it *can* set conditions and safeguards under which data can be exported outside of the EU. By far the most common safeguard to protect exported data in use today is the standard contractual clause—a blanket term for any one of three sets of clauses that must be incorporated verbatim and completely into a contract covering a data transfer. These SCCs specify requirements for both the data importer (the organization receiving the data) and the data exporter (the organization sending it).

The 2020 Schrems II ruling invalidated Privacy Shield, a program for transferring data to the United States, and sharpened the level of scrutiny data exporters are required to apply to their data transfers. In response to that ruling, the European Commission released its new versions of its SCCs. Companies had until September 27, 2021, to update their templates and negotiation playbooks to include the new SCC versions for new contracts. The next step is to amend all executed contracts that contain the old SCCs with the newly released modules by December 27, 2022.[1]

Preparing for repapering projects

The new SCC modules make a number of changes to the structure of SCCs that will affect how organizations need to plan their amendments and, ultimately, result in hefty repapering projects that will need to incorporate the following considerations.

Relationship scope

The previous SCCs covered data transfers from controllers to controllers and from controllers to processors. The updated versions include those scenarios, but also include modules that enable transfers from processors to processors and processors to controllers. This is good news for processors engaging other processors in a subprocessing relationship. Previously, there was no approved mechanism for international subprocessing transfers, making compliance with GDPR impractical. Processors that currently engage subprocessors should isolate their contracts with those subprocessors to identify if and how they might implement these new processor-to-processor SCCs to streamline their data transfer relationships.

Multiparty agreements

The new SCCs contain an optional "docking clause" that enables additional parties to join into the agreement, either as data exporters or as data importers. This offers more flexibility for complex transfers, as any set of SCCs can contain multiple senders and receivers of data. Organizations with complex data transfer arrangements—such as large intra-group data transfers or with multiple entities transferring data to the same organization(s)—may want to review and simplify their contractual requirements by having multiple parties sign on via this docking clause.

Level of detail required

The new SCCs heighten the level of specificity required in the appendices of the SCCs regarding the details of the data being transferred. In particular, data importers must list the specific technical and organizational security measures in place for each data transfer, making it clear which measures apply to which transfers. Organizations repapering their existing contracts must make sure to collect this information in advance to adequately populate these appendices—whether through data mapping or analysis of their executed agreements.

Transfer impact assessments

As a result of the 2020 Schrems II court case, the new SCCs include warranties that both parties have assessed the details of the transfer—including the laws and practices of the destination country, the circumstances of the transfer itself, and the measures of data protection put in place—and determined that they will not undermine the protection of the personal data being transferred.