The Computer & Internet Lawyer

Volume 38 ▲ Number 10 ▲ November/December 2021

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

10 Key Takeaways from the European Commission's New SCCs

By Wim Nauwelaerts

Several months ago, the European Commission announced that it had adopted a new set of standard contractual clauses ("SCCs"). SCCs are standardized and pre-approved model data protection clauses that can be incorporated into contractual arrangements on a voluntary basis, providing an easy-to-implement tool to comply with data transfer restrictions in the EU General Data Protection Regulation ("GDPR").

The role of these SCCs is limited to ensuring appropriate data protection safeguards for international data transfers. The European Commission simultaneously released another set of SCCs that controllers and processors can use to comply with the processor obligations set out in Article 28 of the GDPR.

Wim Nauwelaerts is a partner in the Brussels office of Alston & Bird LLP, leading the firm's European Privacy, Cyber & Data Strategy Team. He may be contacted at *wim.nauwelaerts@alston.com*.

(1) The New SCCs Are More Than Just an Update of the Previous SCCs – They Are an Entirely New Data Transfer Tool

There is general consensus that the previous SCCs – the most recent ones dating back to 2010 – required an overhaul in light of the GDPR's requirements as well as significant developments in the digital economy involving new and more complex data processing activities and multiple parties. However, rather than amending the previous controller-to-controller SCCs and controller-to-processor SCCs, the European Commission decided to create a new set of clauses that will replace all the previous ones. The new SCCs are designed to better reflect today's data transfer realities by covering additional processing and transfer situations and allowing a more flexible approach, for example with the number of parties able to join the SCCs.

At the same time, the new SCCs impose much more onerous obligations on both data exporters and importers with a view to ensuring that the level of data protection guaranteed by the GDPR is not undermined when personal data is transferred outside the European Economic Area ("EEA"). It is therefore safe to say that

the new SCCs set a new and higher benchmark for data transfer tools under Chapter V of the GDPR, which goes far beyond a mere update.

(2) The Previous SCCs Have Ceased to Exist, But There Is an 18 Month Transition Period

The new SCCs entered into force on June 27, 2021, which means data exporters and importers were able to start using the new SCCs from that date. The European Commission decisions implementing the previous SCCs (controller-to-controller and controller-to-processor) were repealed September 27, 2021, which means that the previous SCCs can no longer be entered into. However, data transfer arrangements that were already in place before September 27, 2021 and that are based on the previous version of the SCCs remain valid until December 27, 2022.

Eventually all data transfers based on the previous SCCs will have to be restructured under the new SCCs within 18 months of the new SCCs' coming into force, i.e., by December 27, 2022. Data exporters that fail to ensure a timely migration to the new SCCs without the implementation of another data transfer mechanism risk being held liable for illegal transfers of personal data outside the EEA.

(3) The New SCCs Are Based on a Multifunctional, Modular Approach to Increase Contract Efficiencies

The new SCCs combine general clauses with a modular approach to cater to various transfer scenarios and the complexity of modern processing chains. In addition to the general clauses, data exporters and importers will be able to select one or more "modules" that apply to their situation to tailor their obligations under the new SCCs to their role (as controller or processor) and responsibilities for the data transfer. It is possible for more than two data exporters and importers to sign up to the new SCCs from the start, and through the optional docking clause, additional parties will be able to join the new SCCs as data exporters or importers at a later stage and throughout the life cycle of the contract. In order to join, it will suffice to complete the appendix and sign the relevant annexes to the new SCCs.

Although the new SCCs can (and will most often) be used on a standalone basis, data exporters and importers are free to include the new SCCs in a wider contract and to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the new SCCs or prejudice the fundamental rights or freedoms of individuals.

(4) The New SCCs Have a Broader Scope of Application

The new SCCs are designed to provide appropriate safeguards within the meaning of Articles 46(1) and (2)(c) of the GDPR for the transfer by a controller or processor of personal data processed subject to the GDPR (data exporter) to a controller or (sub)processor whose processing of the data is not subject to the GDPR (data importer). In other words, the new SCCs may be used for data transfers outside the EEA only to the extent that the processing by the data importer does not fall within the scope of the GDPR.

The new SCCs also cover the transfer of personal data by a controller or processor not established in the EEA but whose processing is subject to the GDPR because it relates to the offering of goods or services to individuals in the EEA or the monitoring of their behavior (as far as it takes place within the EEA).

The new SCCs include separate "modules" to cover controller-to-controller and controller-to-processor data transfers, which were already covered by the previous SCCs. However, the new SCCs will also provide coverage to processor-to-processor and even processor-to-controller data transfers – two new transfer scenarios for which industry stakeholders have been requesting a solution for several years.

Another novelty is that when the processing involves international data transfers from controllers to processors, or from processors to subprocessors, the new SCCs should fulfill the requirements of Articles 28(3) and (4) of the GDPR. This means that in those cases, the parties will not be required to enter into or maintain a separate data processing agreement to ensure compliance with Article 28 of the GDPR.

(5) The New SCCs Impose on Data Importers GDPR-Like Principles for Processing Personal Data

To a large extent, the new SCCs mirror the basic data protection principles in Article 5 of the GDPR, which is reflected in extensive obligations for the parties around purpose limitation, transparency for individuals whose personal data are transferred, data minimization, accuracy, and storage limitation. In most cases, the data exporter and data importer will have to make a copy of the new SCCs, including the appendix as completed by them, available to the individuals that have asked for it – free of charge.

In addition, the new SCCs introduce accountability obligations, requiring that each party must be able to demonstrate compliance with its obligations under the new SCCs. Data importers, in particular, will be

required to keep records of the processing activities carried out under their responsibility, which they will have to make available to the relevant supervisory authority on request.

(6) The New SCCs Require Data Importers to Adhere to Data Security Standards That Are Higher Than the Previous SCCs

Under the new SCCs, the data importer and, during transmission, the data exporter will have to implement appropriate technical and organizational measures to ensure the security of the personal data, including protection against personal data breaches. The requirements in the new SCCs are more elaborate than in the previous SCCs, subjecting both the data exporter and the data importer to a higher standard for data security.

Interestingly, the new SCCs also introduce a duty on data importers/controllers to notify the relevant supervisory authority and in some cases affected individuals of personal data breaches. Unfortunately, that notification duty has not been fully aligned with a controller's duty to notify of personal data breaches under Articles 33 and 34 of the GDPR.

(7) The New SCCs Include a Redress and Complaint Handling Procedure for Individuals

Data importers will need to promptly deal with any complaints from individuals about the processing of their transferred data. Data importers may also opt to involve an independent dispute resolution body, at no cost to the individual. Individuals will need to be informed of the redress mechanism and that they are not required to use it. If there is a dispute between an individual and one of the parties over compliance with the new SCCs, that party will have to use its best efforts to resolve the issue amicably in a timely fashion.

Individuals who invoke their third-party beneficiary rights under the new SCCs have the option to lodge a complaint with a supervisory authority or refer the dispute to the local courts. Individuals also may decide to be represented by a not-for-profit body, organization, or association in a dispute concerning the new SCCs.

(8) The New SCCs Include Specific Obligations Aimed at Addressing the CJEU's Concerns in the *Schrems II* Case

The European Commission wanted to make sure that new SCCs provide for specific safeguards in light of the *Schrems II* decision from the Court of Justice of the EU. The new SCCs therefore include elaborate provisions to address the effects of the laws of a third country on the data importer's compliance with the clauses, in particular how to deal with requests from public authorities in that country for disclosure of the transferred personal data.

In essence, the transfer and processing of personal data under the new SCCs should not take place if the laws and practices of the country of destination prevent the data importer from complying with the clauses. To that effect, under the new SCCs both the data exporter and data importer will have to warrant that they have no reason to believe that the laws and practices that apply to the data importer are not in line with these requirements.

According to the European Commission, this requires that the parties conduct a transfer impact assessment that takes account of the specific circumstances of the transfer (such as the content and duration of the contract, the nature of the data to be transferred, the type of recipient, and the purpose of the processing), the laws and practices of the country of destination that are relevant in light of the circumstances of the transfer, and any safeguards put in place to supplement those under the new SCCs (including relevant contractual, technical, and organizational measures). To assess the impact of such laws and practices on compliance with the new SCCs, different elements may be considered, 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 the practical experience of the data exporter and data importer.

If the data importer believes that it is not able to comply with its obligations in the new SCCs, it will have to notify the data exporter, and the latter should identify appropriate measures to address the situation, if necessary in consultation with the relevant supervisory authority. The data exporter may be required to suspend the transfer if no appropriate safeguards can be ensured or if so instructed by the supervisory authority. In some cases, the data importer may also have to notify individuals if it receives a legally binding request from a public authority under the law of the country of destination for disclosure of personal data transferred pursuant to the new SCCs.

More generally, under the new SCCs data importers will be required, at regular intervals, to provide data exporters with aggregate information about data access requests received. The data importer should also document any request for disclosure received and the response provided and make that information available to the data exporter and the supervisory authority

upon request. Data importers will also have a duty to review the legality of requests under the laws of the country of destination and to challenge them if there are reasonable grounds to consider that the requests are unlawful.

(9) The New SCCs Include Strict(er) Rules on Onward Data Transfers

Data importers will find it more challenging to organize onward transfers of the personal data they receive under the new SCCs. Such onward transfers are typically not permitted unless the third party agrees to be bound by the SCCs. Alternatively, onward transfers may take place if the data importer ensures that one of the conditions in Chapter V of the GDPR applies. These include entering into a binding instrument ensuring the same level of data protection as the new SCCs, which is an option that is available in the controller-to-controller module, but surprisingly not in the controller-to-processor module.

Under the processor-to-processor module, the data importer is only allowed to transfer personal data to a third party on documented instructions from the initial controller, as communicated to the data importer by the data exporter. This assumes that processors relying on this module for their data transfers outside the EEA will be able to manage complex instruction chains for all their data controllers, which may be hard to organize in practice.

(10) The New SCCs Require Annexes with More (Detailed) Information About the Transfer

The new SCCs include an appendix with up to three annexes (depending on the modules selected) that the parties will need to complete in order to rely on the new SCCs as a valid data transfer tool. Compared with the previous SCCs, the new SCCs require both the data exporter and the data importer to provide more and more detailed information about the data transfers for which they intend to use the new SCCs. For instance, in addition to listing the parties and their contact details, where applicable, the annexes should include information about the parties' data protection officer and/or representative in the EU, as well as a specification of their role (controller or processor).

The annexes will need to include information about transfer descriptions of the nature of the processing, the purposes of the data transfer and any further processing, the data retention period, and the frequency of the transfer (e.g., whether the data are transferred on a one-off or continuous basis). Furthermore, if the data importer is a processor, a separate annex must be completed if the data exporter has granted a specific authorization to involve subprocessors. In that case, the annex should include a description of processing that includes a clear allocation of responsibilities in case several subprocessors are authorized.

The European Commission has emphasized that it must be possible to clearly distinguish the information that applies to each transfer or category of transfers and to determine the roles of the parties as data exporters and data importers. This implies that, when necessary to ensure sufficient clarity, separate appendices or annexes may need to be used.