BCLP. Client Intelligent

Insights

INTERNATIONAL DATA FLOWS - HOW TO PREPARE FOR THE NEW EU SCCS

May 06, 2021

The last few years have witnessed remarkable changes in the privacy world. The GDPR, the CCPA, the invalidation of the EU-US Privacy Shield framework and the related obligations resulting from the *Schrems II* decision – to name just a few – have left organizations continuously needing to adapt their privacy programs to stay in front of enforcement actions and address new and evolving obligations.

This maelstrom has left organizations with limited bandwidth to implement the new standard contractual clauses ("**SCCs**") from the European Commission. Nevertheless, final publication of these new clauses is imminent (anticipated in May 2021), and the one-year clock for transitioning to the new SCCs will then start ticking. As companies learned during the lead up to the GDPR, CCPA and other new comprehensive privacy laws, a year can pass very quickly. Nevertheless, the message from EU regulators is that they expect companies to make this transition and also continue to take steps to address the requirements established by *Schrems II* sooner rather than later, regardless of the effort involved.

To help organizations approach this daunting process, set out below is a brief description of the new (still draft) SCCs and our recommended steps for preparing for this transition.

The New SCCs – What Companies Need to Know

Although complex, the long-awaited, draft new SCCs are designed to fit better with the realities of the modern digital economy, in particular, the multi-layered, complicated processing chains and multiple exporters and importers of personal data. Unlike the "old" SCCs, which are intended to be implemented separately and only address one type of transfer at a time (controller to controller or controller to processor), the new SCCs are modular in nature to allow companies to address more than one type of transfer using the same framework and also add and remove parties in the future. In addition, two new transfers "options" have been included, which will make it possible to cover some common types of data transfers for which there was no officially, compliant option in the past, such as exports by EU processors.

Specifically, the new SCCs are structured to cover the following types of transfers:

- **Controller to controller**: e.g., between affiliated entities for centralized HR management purposes;
- **Controller to processor**: e.g., between a customer and its payroll or IT vendors/service providers;
- **Processor to subprocessor** (new option): e.g., a SaaS provider (processor) contracting with a third party cloud platform service provider (subprocessor) to provide the service to the (controller) customer;
- **Processor to controller** (new option): e.g., a EU service provider is 'returning' processed personal data originally received from a corporate customer located in a third country.

As currently drafted, the new SCCs also require the parties to carry out and document a **transfer risk assessment**, which must be provided to the competent EU supervisory authority on request. The assessment is essentially an embodiment of certain requirements of the *Schrems II* decision and needs to encompass:

(i) The specific circumstances of the transfer, scale, data types, purpose, etc;

(ii) The relevant laws of the destination country, especially those related to government access and surveillance; and

(iii) Safeguards implemented in addition to the SCCs (e.g., technical and organizational measures, such as encryption).

The importance of the transfer risk assessment was emphasized by the European Data Protection Board ("**EDPB**") and European Data Protection Supervisor ("**EDPS**") in their joint opinion on the draft new SCCs. The EDPB and EDPS recommended that transfer risk assessments should be annexed to the executed new SCCs in order to prevent parties from merely agreeing to document the assessment without actually doing so in practice. Note, however, that it is not currently known whether the finalized SCCs will adopt this recommendation.

Another significant new feature is the obligation in relation to **public authority access requests**. The importer is required to give the exporter prompt notice of any binding access requests received from a public authority, unless prohibited from doing so, and the importer must review the legality of such requests and challenge them where the importer considers there are grounds to do so.

Companies will need to consider whether they can address the obligations set out in the new SCCs (both from an importing and exporting perspective) and will also need to evaluate whether the new SCCs are the best cross-border transfer vehicle for their particular organization. They should continue to monitor other possible mechanisms, such as the potential for a new Privacy Shield for EU-US transfers or Binding Corporate Rules. Nevertheless, the steps described below are intended to help companies that do plan to rely on the new SCCs get ready for them.

How Can Companies Prepare?

Like any significant change, the prospect of transitioning to the new SCCs can leave organizations wondering where to start. The key to making the process as efficient and streamlined as possible is for companies to take the time to prepare to move to the updated SCCs, rather than just assuming this is something that can be achieved quickly by a "repapering" exercise.

Starting the following steps right away will help organizations make this change while also updating and advancing their privacy programs more broadly.

(1) Know your Transfers and your Organization

Identify Current Transfers covered by SCCs: Because SCCs have been around for many years, it is not unusual for companies to have implemented multiple sets across the organization. It will be important for companies to identify, where possible, any existing iterations of the current SCCs that are in use and to formulate a plan for replacing them with the new SCCs.

b. Understand the Roles of the Parties (controller, processor, sub-processor): In addition to identifying current SCC implementations, organizations will need to carefully review their roles with respect to personal data. In particular, the current SCCs do not officially address subprocessor transfers, so organizations have taken a variety of approaches in the past to cover processor to subprocessor transfers. For intragroup or more complicated arrangements, it is likely a combination of the "modules" will be needed, as was commonly the case with the old SCCs being replaced.

c. Refresh Factual Information Relevant to the Transfers: As companies prepare to move from one set of SCCs to the other, they will need to take the time to validate the underlying data flows and update any related factual descriptions. With increasing scrutiny on cross-border transfers, and the emphasis on minimizing data collections and uses in general, organizations should continue to evaluate whether they can justify cross-border transfers of personal data and whether they have appropriately addressed this issue in any refreshed implementation using the new SCCs.

(2) Develop a Consolidated Agreement with Framework Terms

As noted above, the new SCCs are intended to facilitate a broader set of cross-border transfers. To create a truly comprehensive cross-border transfer solution, organizations should take the time to layer on framework provisions that facilitate the update of the agreement, the addition and deletion of parties, the identification of the parties as controllers, processors, subprocessors, and additional terms as needed to address *Schrems II* (discussed below). Companies should also consider whether implementing a Power of Attorney structure to facilitate changes centrally would be a useful, additional step.

(3) Build in *Schrems II* Solution Elements

Organizations should not forget that they still need to address, to the extent possible, the obligations established by the *Schrems II* decision and the related recommendations issued by the EDPB (see our related alert available here). Such steps should, at a high level, include:

a. Local country legal risk assessment.

b. Factual/circumstances-based risk assessment associated with an organization's general industry, data flows, and prior experience with government surveillance demands.

c. As noted above, implementation of appropriate additional contractual protections to be included in the framework agreement.

d. Implementation of existing vendor review process and augmented process for new vendors, with additional *Schrems II* provisions (e.g., restrictions on disclosures to government authorities without notice and consent; implementation of end-to-end encryption, etc.).

e. Implementation of government demands policy or position, as appropriate (i.e., a policy establishing that non-EU companies involved will not provide information to government authorities on a voluntary basis and instead only in response to a valid subpoena or similar, formal request).

f. Implementation of additional technical measures where appropriate (e.g., end-to-end encryption, pseudonymization).

(4) Develop a Review Process to identify factual and legal changes in the future and embed this process in the global privacy program.

Conclusion

The specific path for a company implementing the new SCCs will vary, but all companies will, without a doubt, benefit from an organized approach that avoids rash decision-making, organizational privacy fatigue and resource allocation issues that can plague these kinds of significant projects.

If you would like to discuss any of the above, and how it applies to your organization, please do not hesitate to contact BCLP's Global Data Privacy & Security team.

RELATED PRACTICE AREAS

- Data Privacy & Security