The New Standard Contractual Clauses for Transfers of Personal Data from the EU

On June 4, 2021, the European Commission (EC) issued its long-awaited updated standard contractual clauses (SCCs). The publication of the SCCs is an important moment for the global business community because they allow companies to meet the requirements of the European General Data Protection Regulation (GDPR) when transferring personal data from the European Union (EU) to non-EU countries.

Introduction

As a reminder, the strict GDPR only allows personal data, i.e., all information related to an identified or identifiable living individual, such as employees or customers contact persons, to be transferred outside of the EU if the EC has decided that the receiving non-EU country, a territory or one or more specified sectors within that non-EU country, or an international organization ensures an “adequate” level of protection..

The EC has issued 12 such adequacy decisions so far. Japan is the subject of the most recent adequacy decision (January 2019), and a final decision on South Korea is expected soon. A decision is also expected soon for The United Kingdom, a former EU Member State, which at the end of this month will no longer be able to benefit from the grace period provided by the EU-UK Withdrawal Agreement for international transfers of personal data from the EU.

There have been two tailored adequacy mechanisms for the United States over the years: Safe Harbor and Privacy Shield, but both have been invalidated by respectively the Schrems I and Schrems II decisions of the Court of Justice of the European Union (CJEU).

In the absence of an adequacy decision, parties can implement so-called “appropriate safeguards,” which essentially means that a pre-approved data transfer mechanism is used to protect the personal data. Or, as the EU data protection regulators phrase it, to make sure that the protection of the data travels with the data wherever it goes.

Standard Contractual Clauses

One of the most commonly used “appropriate safeguards” are the SCCs, which are preapproved by the EC and therefore cannot be amended. The GDPR refers to them as “standard data protection clauses adopted by the Commission.”

Up until now, there were three sets of SCCs, two for controller-to-controller transfers adopted in 2001 and 2004 respectively, and another set for controller-to-processor transfers adopted in 2010. Moreover, those SCCs allowed for no flexibility, as each of them had to be used in its entirety.

This one-size-should-but-does-not-fit-all approach has changed with the updated SCCs. While the EC issued its final working document on June 4, 2021, the final, and thus official, version will be published in the Official Journal of the EU shortly, and the final working documents should generally track the final version of the SCCs.

Modernized Approach

The first major change is that the updated SCCs finally refer to the GDPR, which recently celebrated its third anniversary, rather than the outdated former data protection directive.

Second, there is one single, comprehensive set of SCCs instead of separate sets for controller-to-controller or controller-to-processor transfers.

Third, the new approach allows for much more flexibility. As was the case with previous versions of the SCCs, the SCCs cannot be modified, apart from adding or updating information in the annexes of the appendix, but the new SCCs adopt a modular approach where general clauses can be combined with specific clauses to tailor the agreement to the scenario at hand.

Furthermore, while the previous SCCs were drafted to be used between two parties, the new SCCs take a multi-party approach, with the possibility to opt-in by acceding to the SCCs by completing the SCCs' appendix and signing their annex I.A.This allows the entire data processing chain to be covered, as the SCCs can now be used for onward transfers as long as the third party is, or agrees to be, bound by the SCCs. In other words, using the SCCs, personal data can be transferred from the EU to the party in a non-EU country, and then transferred again to another non-EU third party.

Challenges

As mentioned in the article that we published at the end of last year, while these changes may feel like a breath of fresh air when compared to the current version, and should certainly be considered an important improvement, these are arguably not significantly innovative changes from a European contract law point of view.

Furthermore, some additional obligations will certainly be challenging from an operational standpoint. For example, individuals (so-called “data subjects”) should always be informed about the identity of the data importer, which goes a step further than the current transparency obligations stemming from the GDPR, which impose an obligation to inform data subjects about the “categories” of recipients and “the fact” of an (intended) international data transfer.

Additionally, onward transfers are more strictly regulated. Barring a limited number of exceptions such as the consent of the data subject, onward transfers are only allowed to a party that is or agrees to be bound by the SCCs.

Schrems II

One of the key reasons that a draft version of the new SCCs was not published until the end of last year is that the EC was awaiting the Schrems II judgment addressing the legal v validity of SCCs as data transfer mechanism. The SCCs were upheld, but the CJEU ruled that supplementary measures were needed.

The new SCCs take the Schrems II judgment and the subsequent guidance from the European supervisory authorities into account, ensuring that there is no escaping their consequences. Among other obligations, the data importer and/or the data exporter have the following obligations under Section III of the new SCCs:

- Mutual obligation to consider the laws of the data importer’s country: Both the data importer and the data exporter warrant that they have considered the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards. In this context, the new SCCs provide that the parties may consider relevant and documented practical experience of the data importer and the data exporter with prior instances of requests for disclosure from public authorities, or the absence of such requests. Such documented experience should cover a sufficiently representative time-frame as evidenced by internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level. The parties to the SCCs must document this assessment.
- Data importer notification obligation of non-compliance due to laws or practices: The data importer must promptly notify the data exporter if it has reason to believe that it is or has become subject to laws or practices that make it unable for the data importer to comply with the SCCs.
- Supplementary safeguards: To the extent the circumstances in the data importer’s country warrant, the data importer and the data exporter must implement supplementary contractual, technical or organizational safeguards including measures applied during transmission and to the processing of the personal data in the country of destination for

purposes of mitigating risks associated with the transfer.

- Data importer obligation relating to legally binding requests for personal data: The data importer must (i) notify the data exporter about the requests, including information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; (ii) review the legality of requests for personal data; (iii) pursue an appeal; (iv) seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits; (v) not disclose the personal data requested until required to do so under the applicable procedural rules; and (vi) document all of the aforementioned efforts.
- Data importer notification about “direct” access to personal data: This obligation is intended to cover government access, for example in connection with intelligence operations where no “request” for personal data as such is received by the data importer.
- “Best efforts” to fight so-called gag orders: If an obligation to not disclose a request attaches to a government request for personal data, the data importer must engage in documented best efforts to obtain a waiver from such an obligation.

Subject to applicable legal limitations, the data importer and, where applicable, the data exporter must make all of the documentation relating to their compliance efforts available to the supervisory authorities and/or the data exporter upon request. In other words, the SCCs will be part of the “GDPR accountability package” that regulators tend to ask for in case of an inspection and that should allow organizations to demonstrate, and regulators to review, compliance with the GDPR.

Government access to personal data was already a focus point of the Schrems II case, and it remains important in the context of the SCCs too, as the SCCs require the data importer to notify the data exporter “and, where possible, the data subject” in case of a request for or direct access by a public authority, including judicial authorities.

What Should A Company Do Now?

Many organizations have already started (re-)mapping their data transfers. In addition to creating policies, procedures, and other documentation relating to addressing Section III of the new SCCs, those that rely on the previous version(s) of the SCCs will have to adopt the new version within the next 15 months. This is three months longer than the 12 months foreseen in the draft decision, as the previous SCCs will only be repealed in three months, which might be helpful for parties that are currently in the process of signing the old SSCs (which, of course, also require the implementation of supplementary measures imposed by Schrems II).

In summary, the new SCCs provide a more workable instrument for international data transfers than the previous ones, but there is likely more work to be done. It will be “all hands on deck” in the privacy and legal departments of organizations around the world.

Maarten Stassen
Partner – Brussels
Phone: +32.2.214.2837
Email: mstassen@crowell.com
Photograph of Maarten Stassen