PAUL HASTINGS

Stay Current

June 2021

Follow **@Paul_Hastings**

Are the New SCCs Worth the Wait?

By Sarah Pearce, Ashley Webber & Daniel Sullivan-Byrne

As discussed here, the European Commission adopted the new Standard Contractual Clauses (the "**New SCCs**") for transfers of personal data to third countries on 4 June 2021 (the "**Decision**"). The draft version of the New SCCs was published back in November 2020, with many expecting the final version to be adopted a matter of weeks later. However, we were made to wait—six months, no less—so, were they worth the wait? In this article, we will discuss several key takeaways from the New SCCs and provide some general commentary as to their application and suitability. We have also summarised each of the provisions (see here), including which module applies to each clause and whether a clause can be relied upon by a data subject as a third-party beneficiary (discussed further below).

Background of Transfers to the Third Countries and the SCCs

As the reader will likely be aware, the GDPR prohibits the transfer of personal data to a country outside the EU (a "**third country**") unless the third country has been deemed adequate by the European Commission or one of the prescribed transfer mechanisms are in place. One of the mechanisms included in the GDPR are the standard data protection clauses adopted by the Commission (i.e., the SCCs). When the GDPR came into effect in May 2018, the European Commission Decisions 2004/915/EC and 2010/87/EU were in effect and contained SCCs for the transfer of personal data to controllers and processors, respectively, in third countries (referred to throughout this article as the "**Existing SCCs**"). The GDPR expressly states that European Commission Decisions were to remain valid until amended, replaced, or repealed, so therefore the Decisions 2004/915/EC and 2010/87/EU were deemed valid mechanisms for transferring personal data to third countries under the GDPR.

Of course, given the dates upon which the two decisions were adopted, the Existing SCCs did not align with, nor refer to, the GDPR; thus, it was widely accepted that the Existing SCCs were in need of an update. In addition to being outdated from a legislative perspective, the world of data and technology had moved on significantly since the Existing SCCs were prepared, and therefore they simply were no longer reflective of reality. This is acknowledged in the Decision which states that, "*since the decisions were adopted, the digital economy has seen significant developments, with the widespread use of new and more complex processing operations often involving multiple data importers and exporters, long and complex processing chains, and evolving business relationships. This calls for modernisation of the standard contractual clauses to reflect those realities better…*"

In July 2020, the need to adopt new SCCs became even clearer following the Court of Justice of the European Union's decision in Schrems II. Full details of the decision can be seen here, but, to summarise, the Court called into question the effectiveness of the Existing SCCs as a way of protecting personal data transferred to third countries. Based on the Court's analysis, it was clear that new SCCs were required. Schrems II is referred to in the Decision itself and its impact in the New SCCs is discussed further below.

How Do We Use The New SCCs?

The Decision states that the "role of the standard contractual clauses is limited to ensuring appropriate data protection safeguards for international data transfers" and that organisations transferring personal data to third countries are "free to include those standard contractual clauses in a wider contract and to add other clauses or additional safeguards, provided that they do not contradict the standard contractual clauses or prejudice the rights or freedoms of data subjects".

Unlike the Existing SCCs, the New SCCs can be executed by more than two organisations: Annex 1 allows for as many entities to be added as is necessary to reflect the particular transfer of personal data. The New SCCs also contain an optional docking clause, which provides an organisation not party to the SCCs to accede to the SCCs at any time (if agreed upon by the parties), either as a data importer or data exporter, by completing the necessary information in the Appendix and signing the New SCCs. This will likely prove particularly useful for group companies that wish to utilise the New SCCs as an intra-group transfer mechanism.

The New SCCs have introduced the "modular approach". Instead of having several sets of SCCs to cover the different kinds of transfers, the New SCCs capture the following four possible transfers:

1. Module 1: controller to controller
2. Module 2: controller to processor
3. Module 3: processor to processor
4. Module 4: processor to controller

When entering into the SCCs, the parties select the relevant module that applies to their transfer activity and, in addition to the general clauses which apply to all modules, only the clauses which apply to that specific module apply to the parties and the transfer. Please see the summary of clauses here to see which clauses apply to which module. The modular approach is certainly an improvement on the Existing SCCs, as it provides consistency to the parties and, while the new modular approach might seem confusing to some at first, we have seen, with clients implementing the draft versions, familiarity and ease comes with use. Further, the inclusion of modules 3 and 4 is particularly useful as such transfers are not covered by the Existing SCCs.

When Can The New SCCs Be Used?

The New SCCs will become effective 12 days after publication in the Official Journal of the European Union. The Existing SCCs will be repealed three months after the New SCCs are published in the Official Journal. From this date, organisations will not be able to rely on the Existing SCCs for ***new*** data transfers. So for any new transfers after this date, organisations should use the New SCCs.

For data transfers that are currently taking place using the Existing SCCs, they can continue to be relied for such transfers ***until 18 months after*** the New SCCs are published in the Official Journal. This is provided that the Existing SCCs and nature of the transfer are unchanged. See the discussion below in "Next Steps" regarding how organisation should approach replacing the Existing SCCs.

Key Takeaways and Comments

We have summarised below some initial thoughts on the New SCCs.

1. Influence of the GDPR

As noted above, the New SCCs were needed to bring this commonly used transfer mechanism in line with the GDPR. From reading the New SCCs, it is clear that the influence has been vast, as the

language used throughout the New SCCs mirrors that of the GDPR. As the data importer may not be subject to the GDPR, the New SCCs essentially create contractual obligations that mirror regulatory obligations included in the GDPR; this can be seen throughout the New SCCs, but module 1 has some very clear examples with the obligations on the data importer as a controller of the data. See the summary of clauses here.

2. Influence of Schrems II

The Decision states: "In order to provide appropriate safeguards, the standard contractual clauses should ensure that personal data transferred on that basis is afforded a level of protection essentially equivalent to that guaranteed in the Union." The principle of essential equivalence was a key feature of Schrems II; the Court opined that personal data should only be transferred if it could be subject to protections that are equivalent to those provided in the EU (i.e., by the GDPR), and that relying on the Existing SCCs alone would not, in most circumstances, be enough to do this. In such instances, organisations transferring personal data should undertake assessments to identify potential risks and put in place additional safeguards to minimise such risks. This has flowed directly into various clauses within the New SCCs, notably in the security provisions (see further discussion below on security).

Another key focus of the Court in Schrems II was the power of governmental authorities in third countries to request disclosure of, or have access to, the personal data once transferred to that third country. The New SCCs have gone some way to mitigate this risk by including provisions specifically focused on the issue. The aforementioned provisions are most apparent in Section III, entitled "*Local Laws and Obligations in Case of Access by Public Authorities*" and, amongst other things, require that the parties warrant they have no reason to believe the laws and practices in the third country would prevent the data importer from fulfilling its obligations under the SCCs (including by providing access to a governmental authority). There is also a mandated assessment which, as discussed above, was a key message of the Court and has been a consistent part of our advice to clients in this context for some time now. For further details of the provisions, please see the summary of clauses here.

3. Security Obligations

As can be seen in the summary of clauses, there are significant security obligations on all parties in each module. In most instances (except module 4), this requires the parties agreeing technical and organisations measures be implemented by one or both of the parties to protect the data from being subject to a personal data breach. These measures must then be documented in Annex II. In the New SCCs, Annex II contains a non-exhaustive list of examples of security measures, which *could* be used if appropriate for the relevant transfer. There is no indication as to when each such measure should be used, what would kind or nature of transfer would trigger their usage, or what level of risk should be met before a particular measure is implemented, which means the onus is on the parties to make this judgement based on the relevant transfer. For many companies, this will not be a simple task, nor will it be one they necessarily have expertise in. Interestingly, the European Commission press release for the New SCCs stated that they are intended to "*offer more legal predictability to European businesses and help, in particular, SMEs to ensure compliance with requirements for safe data transfers, while allowing data to move freely across borders, without legal barriers*". In our view, SMEs will be most likely to struggle with determining and implementing appropriate measures, given their resources.

Lack of guidance around what are appropriate security measures has often been a criticism from organisations complying with the GDPR and/or utilising the Existing SCCs, and it is likely this will continue based on the information—or lack thereof—in the New SCCs. Following Schrems II, the European Data Protection Board adopted its Recommendations 01/2020 on measures that supplement transfer tools (e.g., the SCCs) to ensure protection of personal data. Whilst the

Recommendations include technical and organisation security suggestions, the suggestions are fairly limited in their application and the guidance provided only goes so far. Indeed, an updated version of the Recommendations is also anticipated in due course. For more information and commentary on the Recommendations, please see here.

For effective application of the New SCCs, further guidance around security measures is required. Whether this comes from European bodies, such as the EDPB or member state data protection authorities, or whether this is something organisations are going to have to invest in themselves, remains to be seen. Market practice will certainly evolve but we would highlight that security has been, and will continue to be, a key focus for data protection regulators and therefore organisations should consider this a high priority.

4. Data Subject Rights

Clause 3 of the New SCCs allows data subjects to "invoke and enforce" certain provisions of the SCCs as third-party beneficiaries against the data exporter and/or data importer. This right is without prejudice to any rights granted to data subjects under the GDPR. For details on which clauses can be enforced, please see the summary of clauses here.

Whilst it is important to ensure data subjects and their privacy remain the focus of organisations when processing personal data, it is questionable how effective this right to invoke and enforce will be without better communicating this message to data subjects themselves. There are transparency obligations on the parties in the New SCCs (which differ between modules) but, from a practical perspective, it is likely that, in most instances, these obligations will be met using the privacy policy of the relevant exporting controller. Whether the message is clear enough, and indeed whether or not the data subject actually reads the privacy policy at all, is currently unknown, and only time will tell.

One thing is clear: for data subjects to fully understand their rights with respect to their personal data under the New SCCs, further guidance tailored to non-specialist individuals is required.

5. Article 28 – Controller/Processor Relationship

According to Paragraph 9 of the Decision, when the transfer is from a controller subject to the GDPR to a processor outside the territorial scope, or from a processor subject to the GDPR to a sub-processor outside the territorial scope, the SCCs "*should also fulfil requirements of Articles 28(3) and (4)*" of the GDPR. As a reminder, Articles 28(3) and (4) are those provisions that require an agreement containing specific, prescribed rights and obligations be entered into by organisations in a controller/processor or processor/sub-processor relationship, commonly referred to as a "data processing agreement" or an "Article 28 DPA". The New SCCs have, therefore, been drafted in such a manner that they contain the specific rights and obligations required by Article 28. For some organisations (possibly SMEs as noted in the Decision), this could remove a cumbersome burden of negotiating a separate and additional DPA if required under Article 28. However many organisations, particularly the larger organisations, will not welcome this approach, as they will prefer to rely on their standard form DPAs which are tailored to their business, services, etc.

Going forward, when using the New SCCs for a processor or sub-processor based in a third country alongside a DPA, it would be good practice to acknowledge in the DPA or other contract that the SCCs are being utilised with respect to the transfer only and Article 28 requirements are being met using the DPA.

6. The UK Position

Whilst transfers from the UK can currently utilise the Existing SCCs to transfer personal data outside the UK/EU, the New SCCs will not automatically be able to be used in connections with data transfers

from the UK. However, it is expected that the Information Commissioner's Office will adopt a similar set of clauses for data transfers from the UK in due course, reportedly during the course of 2021.

Summary of Clauses

We have summarised each clause in the table accessible here. The table provides a brief description of the obligations/rights of the parties under each clause, but, for full details on applicable obligations/rights please review the New SCCs.

When reviewing the clauses in the table, you will see we have identified which module(s) apply to each clause. We note that certain clause headings are repeated in the New SCCs for *different* modules (for example, see the sub-clauses in Clause 8) and would flag that when utilising the New SCCs, it is important to be alert to the relevant module which applies to the transfer in question and to ensure the correct clauses are implemented.

Next Steps

The adoption of the New SCCs is to be welcomed, as they are significantly more suited to the current data protection regime and data sharing practices. They also take into account certain of the key concerns highlighted by the Court in Schrems II, which will hopefully, in turn, ensure better protection for personal data globally.

That said, the adoption will also bring with it a potentially substantial international transfer and contractual review project. Some organisations may have a head start on this if they took steps following Schrems II. However, many opted to wait for the adoption of the New SCCs and for further guidance from regulators and other bodies to ensure they fully understood the expectations and requirements before beginning such a project. Now, given the adoption of the New SCCs, all organisations transferring personal data from the EU/U.K. to third countries should conduct such a review project.

The following is a high level summary of some of the actions which may be required in a project of this nature:

1. **Project Team**: To effectively conduct a project of this size, it is important that the project is staffed by those members of the organisation who will be best suited to assist. Depending on the nature of the organisation, this may include staff located in jurisdictions all over the world and should include a variety of practice areas including privacy, legal, HR, product specialists, and IT.

2. **Mapping**: Arguably, the most important (and likely most time consuming) step is mapping the data flows. This means identifying when personal data is transferred to third countries, either to third-party organisations or on an intra-group basis. Note that this should also include any onward transfers (e.g., if a third-party vendor in a third country transfers the personal data to a sub-vendor in another third country). A thorough and accurate data map will make this project significantly easier.

3. **Transfer Mechanism**: As part of the mapping process, the mechanism currently relied on to transfer the personal data should also be recorded. Most important here is to identify when the Existing SCCs are relied upon and when there is no valid mechanism relied upon at all.

4. **Assessment**: Unless undertaken previously (possibly following Schrems II), an assessment of each transfer should be carried out with the data importer. As noted above, an assessment is now mandated in the New SCCs and was a key message from Schrems II.

5. **New SCCs**: Where required, execute the New SCCs. It is crucial that the information included in the Appendix accurately reflects the transfer taking place: it should not be assumed that the information in the existing executed SCCs (if in place) is correct.

We are already assisting clients with projects of this nature, gaining and developing in-depth experience in the area and helping to drive market practice. As noted above, there will be roughly an 18-month period to replace all Existing SCCs with the New SCCs; in theory, this is ample time, but for global organisations that regularly transfer personal data for various reasons (be that with vendors or other third parties), across multiple jurisdictions, this will take time. Our suggestion therefore would be to start this project as soon as possible to ensure the deadline is met.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings London lawyers:

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Ashley Webber
44.020.3023.5197
ashleywebber@paulhastings.com

Daniel Sullivan-Byrne
44.020.3023.5174
danielsullivanbyrne@paulhastings.com