New Standard Contractual Clauses – Dentons' initial analysis

June 10, 2021

On June 4, 2021, the European Commission (**EC**) published its long-awaited final Implementing Decision adopting new Standard Contractual Clauses (the "**New SCCs**") for the transfer of personal data to third countries. On November 12, 2020, the EC had published a draft implementing decision for public consultation (the "**Consultation Draft**"). The new SCCs are the European Commission's answer to personal data exports in the post-GDPR, post Schrems II world, and have been much anticipated by the privacy community. They come into effect on June 27, 2021 (i.e. 20 days after their publication in the EU's Official Journal, on June 7, 2021).

This client update provides our initial key observations and highlights the material differences between the Consultation Draft and the New SCCs. We have also prepared a redline comparison between the Consultation Draft and the New SCCs, which is available for download here.

Key observations

- **Modular approach**: The structure of the New SCCs is very similar to the Consultation Draft, in that it still follows the modular approach introduced in the Consultation Draft. Four transfer scenarios are included:
  - Controller-to-Controller (Module One)
  - Controller-to-Processor (Module Two)
  - Processor-to-Processor (Module Three)
  - Processor-to-Controller (Module Four)

  Between them, they should cover most if not all possible transfer scenarios; especially if we take into account the new geographical scope.

- **Application to companies outside the EU**: The New SCCs expressly recognize that the data exporter can be established outside the EU. This is important, because exporters that are subject to the GDPR under Article 3(2) can use the New SCCs, for example a non-EU based controller or processor can enter into the new SCCs with their processor or sub-processor (thereby plugging a major gap in the previous SCC regime). At the same time, however, the new SCCs could also be interpreted as suggesting that they cannot be used with a data importer who is already subject to the GDPR by virtue of the GDPR's extra-territorial application based on Article 3(2) (see new SCCs implementing decision Article 1 and Recital 7). Hopefully, further guidance will clarify this point.

- **Multi-party SCCs**: The new SCCs enable multiple parties to enter into the new SCCs, and also set out a docking clause mechanism which allows for new parties to be added over time. Although in practice parties would often follow such approaches in their arrangements under the old SCCs, for example in intra-group data transfer

agreements, this was not a legally "bullet-proof" practice as there were some question marks around this in certain quarters. The new SCCs now clarify this issue.

- **No separate data processing agreement**: Modules Two and Three of the New SCCs contain all the requirements from Article 28 GDPR, meaning that in case of controller-to-processor and processor-to-processor transfers, no additional data processing agreement is needed. This will save paperwork and avoid inconsistencies between the data processing agreement (which often is a template) and the New SCCs.
- **Liability**: The New SCCs state: “each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses” (Clause 12). It is not clear if parties may amend this provision, e.g. to shift the liability to one of the parties, or to limit liability. While parties are allowed to add other clauses as long as they do not directly or indirectly contradict the New SCCs or reduce the data subjects’ protection granted by the New SCCs (Clause 2(a)), a key open question is if limiting liability between the parties can be considered to contradict Clause 12. We should expect this area to remain contested and a key negotiation topic.

… and material differences

- **Extended transition period**: The New SCCs allow organizations to continue to use the “old” SCCs for new transfers until September 27, 2021. Further, organizations can use the “old” SCCs for existing transfers for a period of up to 18 months, giving parties until December 27, 2022, to transition over to the New SCCs.
- **Relevant modules suffice**: Parties are allowed to select the relevant module(s) only and do not have to incorporate the entirety of the New SCCs including modules that do not apply. This is a useful addition to the New SCCs, making them more user-friendly.
- **Providing information to data subjects**: The Consultation Draft already provided that parties to the SCCs must provide a copy to the data subjects upon request, with redactions being allowed to protect business secrets and other confidential information. The New SCCs add that the parties must provide the data subject with the reasons for the redactions (without revealing the redacted information of course). This is another clear indication that the New SCCs very much require a tailored approach by the parties and that the days of “box-ticking” exercises are over.
- **Module 3 information obligations**: In Module Three there appear to be some inconsistencies in the way the data importer (i.e. the sub-processor) must provide information.

- Clause 8.4 provides that the data importer should inform the data exporter if it discovers the data is inaccurate or has become outdated. The Consultation Draft reads here that the controller should be informed too. This may create problems in practice, as often there is no direct contact between a controller and a sub-processor (e.g. a SaaS provider using a third- party cloud storage vendor), so the change in the New SCCs makes sense.
- However, in Clause 9 (the use of sub-processors) Module Three under (a) requires the data importer to inform and obtain consent from the controller before it may use or change a sub-processor.
- Interestingly, the subsequent sub-clauses then again seem to go from the position that the data importer liaises with the data exporter (which in Module Three is the processor) instead of the controller. See for example sub-Clauses (d) and (e), and to some extent also (c). Compare further Clause 15 (b), which requires the data importer to make its legal assessment of a government access request available to the data exporter, regardless of the applicable module; for Module Three, the New SCCs explicitly state that the data exporter makes available this assessment to the controller.
- Further guidance on this topic would be welcome.

- **Use of sub-processors**: Processors and sub-processors seeking to subcontract (a part of) their processing activities (or change a subcontractor) must have authorization from the data exporter (or the controller – see above). When asking for this consent – and this is new compared to the Consultation Draft – they must provide the information necessary for the data exporter / controller to decide on the authorization. This is another provision that clearly signals the mind shift the New SCCs bring.
- **Schrems II**: The elephant in the room is of course “Schrems II”. We have all been curious to see how the EC would implement the outcome of the Schrems II into the New SCCs.
  - In the Consultation Draft, the EC already introduced a risk-based approach (as opposed to the EDPB in its draft supplementary measures recommendations). In the New SCCs the EC stuck with this approach and even expanded it. The New SCCs provide that parties have to carry out a data transfer impact assessment, document this, and make it available to the competent supervisory authority upon request. When undertaking their data transfer impact assessment, the parties may take into account “relevant and documented practical experience with prior instances of request for disclosure from public authorities, or the absence of such requests”. This is qualified by an extensive footnote setting out further requirements, but nonetheless this is positive news for organizations that have never received any government access requests for data in practice and which, given the nature of their organization and the data they hold, are unlikely to receive such requests. Could this be a preview of what we can expect from the EDPB final supplementary measures recommendations?
  - The Consultation Draft already included the obligation for the data importer to challenge government access requests if there are reasonable grounds for doing so. The New SCCs maintain this obligation in Clause 15 and add some further guidance and specifications, for example the obligation to pursue possibilities of appeal where reasonable. The data importer must document its legal assessment and make this available to the data exporter (and the competent supervisory authority upon request). The requirement to challenge government access requests is likely a welcome development for those data importers who are already taking (or promoting) this approach, however it will likely be onerous for others as it essentially forces importers into litigation with government authorities
  - Beyond these changes, the New SCCs broadly follow the Consultation Draft. They incorporate a number of the EDPB recommendations, including the requirement to document requests and the requirement for processors/importers to implement strict access controls. Furthermore, Annex II (technical measures) mirrors a number of the EDPB’s recommendations, including references to encryption and pseudonymization.

- This issue would never have a perfect solution. But at least it looks like the new SCCs strike a good balance between the requirements of Schrems II and the operational reality on the ground, seem to be aligned with the developing de facto market practices, and seem to have avoided the most conservative positions that have been advocated since the CJEU handed down its judgment in Schrems II last summer.

- **Annexes.**
  - The New SCCs have three annexes:
    - Annex I should set out the parties, a description of the transfer, and (for Modules One, Two and Three) the competent supervisory authorities;
    - Annex II should contain the technical and organizational security measures to ensure an appropriate level of protection;
    - Annex III should have the list of approved sub-processors (Modules Two and Three only).

  - The New SCCs have explanatory notes for each of these Annexes clarifying that the information provided should be "specific and not generic". If the New SCCs are used to cover multiple (categories of) data transfers, the annexes should "clearly distinguish the information applicable to each transfer or category of transfer". If it is not possible to do this in one combined annex, they should be separated.
  - Annex II includes a long list of possible security measures and organizations are expected to provide meaningful and specific information. This is a departure from the current practice where security measures are often described in generic terms. If sub-processors are involved, Annex II should include the specific technical and organizational measures these sub-processors will take to be able to provide assistance to the data exporter / controller.
  - Annex III now requires a description of the processing activities undertaken by each sub-processor, including a clear delimitation of responsibilities if multiple sub-processors are used. Processors can thus no longer suffice by simply listing their sub-processors; they will have to provide real context.

All in all, the approach that the new SCCs set out for populating the annexes will require parties to the SCCs to develop and be able to reflect in the annexes a more detailed and granular understanding of the operational details of the data processing activities than is currently common practice.

As far as the UK is concerned, the new SCCs are not required for exports of personal data from the UK. For now, UK data exports may continue on the basis of the existing SCCs, at least until the UK ICO publishes guidance that encourages the adoption of the new SCCs or (more likely) the UK promulgates its own SCCs. With the consultation regarding the new UK SCCs expected in the summer, it would be interesting to see the extent to which the new UK SCCs will deviate from the new EU SCCs (and if so in which areas and to what degree) or whether the UK government will keep such deviations to a minimum or recognize that the new EU SCCs can be used instead of the new UK SCCs to help minimize the situations in which a data exporting organization will need two different SCCs (one for the UK and one for the EU) for the same data exporting activity. In relation to transfers from the EU to the UK, the entire European economy is currently holding its breath ahead of the European Commission's final decision on UK adequacy.

Much more can be said about the new SCCs. The Dentons' global Privacy and Cybersecurity Group will continue to digest the New SCCs and how they work (or do not work) in practice, and client reactions and approaches to them, and we will be publishing further guidance in due course.

In the meantime, organizations that have postponed taking concrete actions while the SCCs were still in draft now have to start preparing for the transition in earnest. Given the much more tailored approach, this is no mean feat and we recommend starting sooner rather than later. December 27, 2022, seems very far away, but if you have to map, review and negotiate hundreds or even thousands of contracts you will need every day to get this across the line in time. Please reach out to any of the contacts listed below or your usual contact at Dentons if you would like to find out more.

Your Key Contacts

Chantal Bernier
Of Counsel, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Simon Elliott
Partner, London
D +44 20 7246 7423
simon.elliott@dentons.com

Nick Graham
Partner, London
D +44 20 7320 6907
M +44 7795 618 315
nick.graham@dentons.com

Giangiacomo Olivi
Partner, Milan
D +39 02 726 268 00
M +39 344 27 62 550
giangiacomo.olivi@dentons.com

Todd D. Daubert
Partner, Washington, DC
D +1 202 408 6458
M +1 202 436 1819
todd.daubert@dentons.com

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

Tatiana Kruse
Of Counsel, London
D +44 20 7320 6153
tatiana.kruse@dentons.com

Antonis Patrikios
Partner, London
D +44 20 7246 7798
M +44 7919 491029
antonis.patrikios@dentons.com