STEPHENSON HARWOOD

Map, Update, Remediate

What do the European Commission's new Standard Contractual Clauses mean for you?

On 4 June 2021, the European Commission adopted new standard contractual clauses for transfers of personal data to third countries ("**New SCCs**"), which are set to come into effect on 27 June 2021 (i.e. 20 days after they were published in the Official Journal of the European Union). The New SCCs will replace both sets of the Commission's current standard contractual clauses ("**Old SCCs**"), which are now over a decade old.

Since then, the EU's data protection regime has undergone a huge transformation, with the introduction of the EU General Data Protection Regulation (the "**GDPR**") in 2018 and, more recently, the decision of the Court of Justice of the European Union ("**CJEU**") *in Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, C-311/18* ("**Schrems II**") in July 2020. The New SCCs cover these developments and, as a result, place more onerous obligations on both data exporters and importers.

The New SCCs may be used from **27 June 2021** and **must** be used in place of the Old SCCs where parties enter into new transfer arrangements from **27 September 2021**, following a three-month transition period. Where ongoing transfers are already underway prior to 27 September, parties may still rely on the Old SCCs for a further 15 months until **27 December 2022**, provided that details of the processing do not change and that appropriate safeguards for the transfer are otherwise provided.

This update sets out the scope and applicability of the New SCCs and identifies some of the key changes compared to the Old SCCs. It also recommends steps you can take to prepare for the New SCCs.

How do the New SCCs work?

Like the Old SCCs, the New SCCs should be used as a safeguard under Article 46(2)(c) of the GDPR where personal data is being transferred from the European Union to a jurisdiction outside of the European Economic Area ("**EEA**") that does not benefit from a Commission adequacy decision under Article 45(3) (a "**Restricted Transfer**"). Note that the Commission **also** published standard contractual clauses for optional use in contracts between controllers and processors where there is no Restricted Transfer on the same date, which this update does not cover.

The modular format of the New SCCs means that they cover more transfer scenarios than the Old SCCs. As with the Old SCCs, the New SCCs provide for transfers from controller to controller and controller to processor, but now they also cover transfers from processor to (sub-)processor and from processor back to its controller. This flexibility means that the New SCCs will far more transfer scenarios with greater ease.

Where the controller to processor module is used, the New SCCs contain built-in provisions covering the Article 28 GDPR requirements for such contracts, which means that there is no legal obligation to cover these elsewhere. There are still sound reasons to enter into additional terms covering commercial points that are not included in the New SCCs, such as who pays the cost of audits and around indemnities and liabilities. As the New SCCs permit the exporter to terminate transfers if it considers that the importer cannot ensure there are appropriate safeguards in place for the export, importers may wish to consider protective provisions if this termination right is exercised by an exporter keen to exit a long-term commercial relationship. Additional provisions, or accompanying terms, are permitted provided that they do not contradict the New SCCs.

Additional flexibility is provided by "docking" clauses that allow a party to sign up to any of the roles in the New SCCs during the life of the contract. This is something that many organisations were already doing where group structures or service providers or recipients changed, but it's a welcome addition to the content of the SCCs themselves. The mechanics of docking are not spelled out – the SCCs merely say that a new party may accede "by agreement of the Parties", by completing a new data transfer Appendix and signing Annex I.A. It is not clear how the existing parties would give agreement, so this may need to be covered in additional terms.

What transfers do (and don't) the New SCCs cover?

The New SCCs state that they may be used where the exporting party **is subject to the GDPR** (whether based in the EU or not) and the importer for a Restricted Transfer is **not subject to the GDPR**[1]. This resolves a key issue with the Old SCCs, namely that they were drafted on the assumption that the exporter was established in the EU.

The New SCCs state that they may be used only to the extent that the importer's processing falls outside the scope of the GDPR. This is significant: if an importer is subject to the GDPR (under its Article 3(2) extra-territorial scope) then, on the face of it, it appears that New SCCs would not be appropriate to safeguard that transfer. This would make sense, as to require importers subject to the GDPR to sign up to the New SCCs would be to reiterate many of their pre-existing legal duties in contractual form. We'd welcome more clarity over whether (and which) alternative safeguards should be applied in this situation, or whether such transfer is considered a GDPR Restricted Transfer at all. It appears that the European Data Protection Board ("**EDPB**") is considering this point and will be addressing it in upcoming guidance.

In any event, is likely that any Restricted Transfer would still require a transfer impact assessment ("**TIA**") to assess whether the destination country's laws offer essentially equivalent protection and whether any supplementary measures are required, whether or not the New SCCs apply. See further below for what the New SCCs require on TIAs.

What about exporters under the UK GDPR?

Following the UK's withdrawal from the EU, the New SCCs will not automatically apply to data exports that are subject to the UK GDPR. The Information Commissioner's Office (the "**ICO**") has confirmed that it will consult on the UK's own standard contractual clauses over this summer and it is likely that these New SCCs will be influential in that process. The ICO has stated that the Old SCCs are a valid method of safeguarding UK GDPR data exports (with limited UK-specific amendments permitted). However, it has not confirmed the same in relation to the New SCCs. This means that there is potential for a transfer subject to both the UK and EU GDPR to require two sets of SCCs to safeguard it. Many multi-nationals will be hoping that the ICO takes a pragmatic approach here.

[1]Recital 7 to the Implementing Decision of the New SCCs

Do the New SCCs solve all our *Schrems II* problems?

The New SCCs incorporate some new provisions that are clearly influenced by the *Schrems II* judgment. In particular, they anticipate that a risk assessment (or TIA) will be carried out and documented for all transfers relying on the New SCCs, such that parties can assess whether exported personal data will be offered essentially equivalent protection and whether any additional safeguards should be implemented.

Under the New SCCs, parties must warrant that they have no reason to believe that the applicable laws and practices in the country of destination will prevent the importer from fulfilling its obligations under the New SCCs. Local laws that are consistent with the objectives in Article 23(1) of the GDPR are likely to be considered acceptable. The New SCCs require the parties to take the following factors into account in giving this warranty, which would therefore form a key part of the parties' TIA:

- ✓ **The specific circumstances of the transfer,** including the number of entities in the processing chain and transmission channels used; **intended onward transfers; the type of recipient**; the **purpose of processing;** the **categories and format** of data; the relevant economic **sector; and the storage location** of the transferred data.
- ✓ **Laws and practices of the third country of destination**, including those requiring the data to be disclosed to, or authorising access by, public authorities, as relevant to the specific circumstances of the transfer and applicable limitations and safeguards.
- ✓ Any relevant **contractual, technical or organisational safeguards** that supplement the New SCCs.

In considering the laws and practices of the destination country, the New SCCs state that parties may rely on their "practical experience" of public authority access to data, as long as this is "supported by other relevant, objective elements", such as publicly accessible and reliable information. This move towards a risk-based approach will be welcomed by many exporters and importers. We await the EDPB's reaction to this approach in the final version of its draft guidance from November 2020.

The New SCCs also place onerous obligations on importers to ensure access requests and access by public authorities are kept to a minimum and, where possible, notified to exporters and data subjects. Where a public authority access request is received, importers will need to assess their ability to challenge or suspend the request, limit the amount of data disclosed; and document the request and assessment.

The New SCCs also address the issue of onward transfers and require parties to apply appropriate safeguards to those transfers too. Importantly, the TIA must also assess any intended onward transfers. If acting as an importing controller, the New SCCs now require to notify the affected data subjects of specific details about your intended onward transfers, including the purpose of those transfers and the grounds you intend to rely on to make such transfers.

What do I need to do next?

(Re)map your transfers

Many organisations have been mapping their transfers and carrying out TIAs in an effort to comply with *Schrems II*. The outputs of any mapping exercise and existing TIAs may need to be reviewed in light of the risk assessment provisions in the New SCCs, plus their distinction between importers that are subject to the GDPR and those that are not.

Align your data protection documentation with the New SCCs

New data processing terms aligned to the New SCCs must be ready to be rolled out from **27 September 2021** at the latest. Therefore, beginning immediately, entities that use the New SCCs should review their data processing agreements and standard terms to ensure that they do not conflict with the drafting of the New SCCs.

This is necessary because the New SCCs cover very similar ground to many other data processing contracts, such as the Article 28 obligations on processors and obligations around breach notifications, transparency and appropriate technical and organisational measures. To the extent that these conflict with the New SCCs, they will need to be changed and made consistent, as the New SCCs must prevail.

The three-month transitional period to 27 September allows for time to adjust terms before the New SCCs become mandatory for new Restricted Transfers and the Old SCCs are repealed. This means that any contracts being negotiated that may sign after September should look to incorporate the New SCCs now.

Remediate transfers relying on Old SCCs

Organisations will need to remediate all of their ongoing Restricted Transfers that currently rely on the Old SCCs as a safeguard, at the latest by **27 December 2022**. This could be a considerable task for many entities, as they will have just 18 months to complete a large repapering exercise. After this, the Old SCCs will be completely redundant and will no longer provide an appropriate safeguard for international transfers.

While the onus will be on exporters subject to the GDPR to push to remediate their transfer terms, there will also be considerable pressure on importers to respond in time, particularly large importers that operate under standard terms. Intra-group transfers and transfers to vendors, customers and other third parties must all be considered.

Ensure you can practically comply

While rolling out the New SCCs and replacing the Old SCCs is a task in itself, exporters and importers also have a significant job to do in verifying that they can actually comply with their requirements. For importers not subject to the GDPR, this may mean conducting a complete GDPR compliance overhaul and putting in place measures such as notices and procedures in order to comply with the GDPR principles.

In practice, if you are already subject to the GDPR, moving to the New SCCs is unlikely to require too many changes to your current internal compliance practices. However, remember that there will still be a need to undertake TIAs for Restricted Transfers following *Schrems II*. This means that procedures should be updated to ensure that all Restricted Transfers undergo a TIA, and that the results are implemented, and any supplemental measures adopted, regardless of any reliance on the New SCCs.

What's new? Key differences between the New SCCs and the Old SCCs

Provision of New SCCs

Transparency: Controller to Controller module: Section II, Clause 8.2(a)
Importers must inform data subjects (either directly or through the exporter) of their identity and contact details, the categories of personal data processed, the identity of any third party recipients and the purpose of the transfer.

No such requirements are placed on importers acting as processors.

Breach Notification: Controller to Controller module, Section II, Clause 8.5(e) - (f)
Where an importer acting as a controller suffers a personal data breach in relation to transferred data it must notify the exporter and supervisory authority of the breach without undue delay if the breach poses a risk to rights and freedoms. The importer must also notify data subjects themselves where there is a high risk to the rights and freedoms of people. This is in line with the obligations set out in Article 33 and 34 of the GDPR, albeit without the 72 hour time limit.

Onward Transfers: Controller to Controller module, Section II Clause 8.7
Importers may only make an onward transfer if the recipient of the onward transfer agrees to be bound by the New SCCs or if certain other grounds are met, including the third country benefits from an adequacy decision, the parties ensure appropriate safeguards under Art. 46 and 47 of the GDPR, the parties enter into a binding instrument, it is necessary for legal claims or vital interests or (as a last resort) based on explicit consent.

Controller to Processor module and Processor to Processor module, Section II, Clause 8.8
Importers acting as processors may only make an onward transfer on the instructions of the exporter. The grounds for making an onward transfer are reduced under these two modules, meaning processors cannot rely on binding instruments or explicit consent.

Documentation: Controller to Controller module Section II, Clause 8.9; Controller to Processor module Section II, Clause 8.9(b) and (c); Processor to Processor module, Section II, Clause 8.9(b) and (c)

Importers must keep appropriate documentation of the processing activities carried out under its responsibility and make such documentation available to the competent supervisory authority (in the case of controller importers) or the exporter/controller (in the case of processor exporters) on request.

Sub-processors: Controller to Processor Module, Section II, Clause 9, Processor to Processor Module, Section II, Clause 9
Any party acting as a processor that wishes to engage sub-processors must enter into a sub-processing agreement and the controller must provide consent for such sub-processing in the form of either (i) specific authorisation prior to the engagement of a sub-processor or (ii) by general written authorisation.

Key change from Old SCCs

Transparency: There were no requirements in the Old SCCs for controller importers to ensure that data subjects are given this information.

Note that, even where the transfer is to a processor, the New SCCs still require the exporter to make a copy of the SCCs available, although it may redact parts of the Appendix to the extent necessary to protect business secrets or other confidential information.

Breach Notification: Importers acting as controllers were not previously required to notify data breaches under the Old SCCs. They are now faced with the potential for much more direct contact with supervisory authorities and data subjects, in relation to breaches and otherwise.

Onward Transfers: Under the New SCCs, there is no requirement for an importer acting as a controller to notify the exporter of intended onward transfers

The Old SCCs placed the burden on the controller to ensure adequate safeguards were in place for onward transfers. Importing processors must now take steps themselves to ensure any onward transfer offers adequate protection for the transferred data.

Documentation: There was no specific requirement for importers to maintain adequate documentation under the Old SCCs, meaning importers will have to maintain similar records to those required under the GDPR.

Sub-processors: The requirement to obtain the controller's consent for sub-processing has been aligned with the GDPR and is more flexible than the strict prior consent requirement under the Old SCCs.

What's new? Key differences between the New SCCs and the Old SCCs

Provision of New SCCs	Key change from Old SCCs
Data Subject Rights: Controller to Controller module, Section II, Clause 10 Importers are required to comply with requests for access, erasure and objections to processing for direct marketing purposes and offer data subjects the option to contest automated decisions. This is different under the other modules, in particular under the Controller to Processor and Processor to Processor modules, where importers are only required to notify exporters of any data subject requests and assist exporters in complying with these requests.	**Data Subject Rights:** Under the Old SCCs, the importer was only responsible for responding to data subject requests if that was explicitly agreed with the exporter. This means importers otherwise not subject to the GDPR will have to comply with data subject rights.
Assessment of Local Laws: All modules, Section III, Clause 14(a) and (b) Importers are required to assist in the assessment of the destination country's legislation, particularly around public authority access. **All modules, Section III, Clause 14(e)** Importers are required to notify exporters of any relevant changes to such laws.	**Assessment of Local Laws:** The Old SCCs included a warranty by the importer that it had no reason to believe that applicable local legislation would prevent it from fulfilling complying with its obligations but the New SCCs go further by requiring an active assessment to be carried out. The parties still warrant that they have no reason to believe that local laws and practices in the importer's country would prevent the importer from complying with its obligations under the New SCCs. However, the new SCCs explicitly allow the parties to rely on their "practical experience" of public authority access to data, as long as this is "supported by other relevant, objective elements".
Inability to Comply: All modules, Section III, Clause 14(f) If an exporter believes an importer can no longer comply with the New SCCs, it must assess the transfers. If additional safeguards may assist, the exporter **must** apply them or if there are no adequate safeguards they **must** cease the transfer.	**Inability to Comply:** There are additional requirements in light of *Schrems II* requiring ongoing assessment of the data protection laws in destination countries.
Public Authority Access: All modules, Section III, Clause 15.1 Importers must promptly notify the exporter and data subjects of any public authority access request. **All Modules, Section III, Clause 15.2** Importers must review the legality of any such requests and document its assessment.	**Public Authority Access:** The New SCCs place an additional burden on importers not only to inform exporters and data subjects about government access requests but also to try and prevent disproportionate access. This is in line with *Schrems II*.
Governing Law: Controller to Controller module, Controller to Processor module, Processor to Processor module, Section IV, Clause 17 The parties may choose the governing law of any member state that allows for third party beneficiary rights. **Controller to Processor module, Processor to Processor module, Section IV, Clause 17** There is an additional option for these two modules which allows the parties to select the law of the member state in which the exporter is established, provided third-party beneficiary rights are allowed under that law.	**Governing Law:** The Old SCCs were governed by the law and courts of the Member State in which the exporter is established by default.
Technical and organisational measures: All modules, Annex II The Parties are required to provide a detailed description of technical and organisational measures implemented in Annex II. This description is to be specific and not generic and demonstrates a renewed focus on cybersecurity.	**Technical and organisational measures:** Under the Old SCCs, there was no requirement to describe specifically (as opposed to generically) the technical and organisational security measures put in place.

GET IN TOUCH

Katie Hewson

Partner, data protection

T: +44 20 7809 2374
E: katie.hewson@shlegal.com

Olivia Fraser

Associate, data protection

T: +44 20 7809 2844
E: olivia.fraser@shlegal.com

www.shlegal.com

STEPHENSON HARWOOD

BD1202-SSC-0621