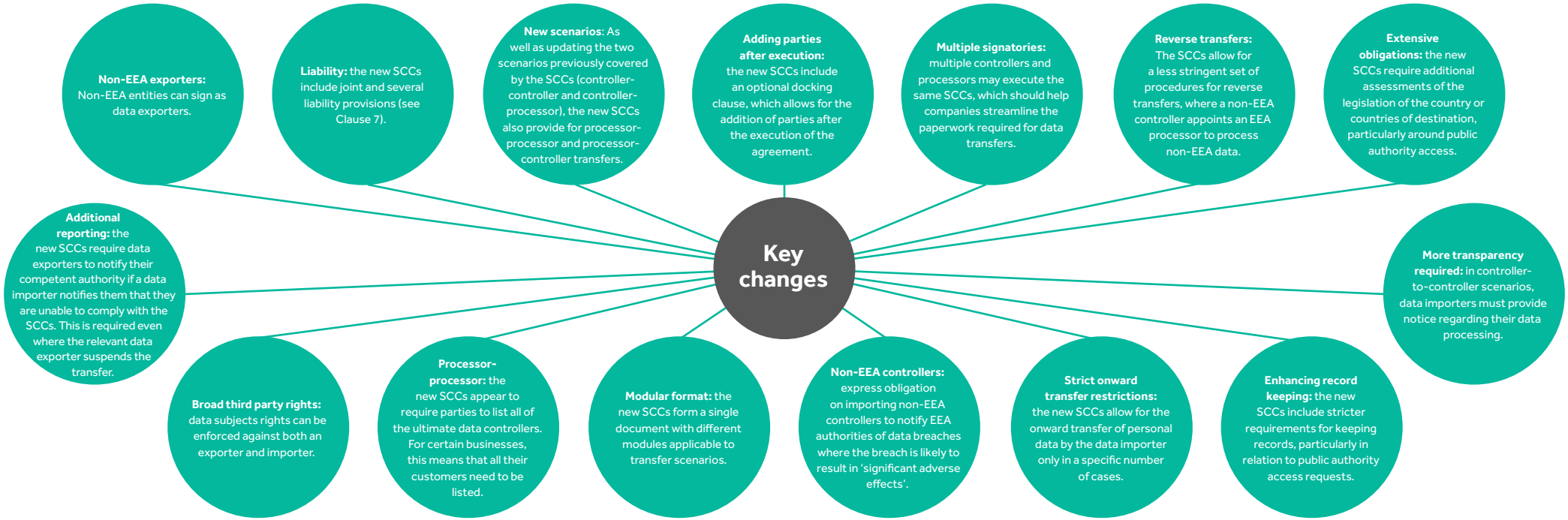
STEPHENSON HARWOOD

Standard contractual clauses: Updating transfer mechanisms in a post-***Schrems II*** world

On 12 November 2020, the European Commission published a draft of the new standard contractual clauses, which are used to safeguard transfers of personal data from the European Economic Area (the "**EEA**") to third countries (the "**new SCCs**"). The clarity of the new SCCs is a significant improvement on the previous 2001, 2004 and 2010 SCCs. The new SCCs update the clauses for the General Data Protection Regulation ("**GDPR**"), plus address the issues arising from the decision of the European Court of Justice ("**CJEU**") in July 2020 in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, C-311/18* ("***Schrems II***"). Once the new SCCs are finalised and officially adopted (expected in early 2021), there will be a one-year period before the old versions are repealed. We have summarised some of the key changes introduced by the new SCCs, considered how they address ***Schrems II***, and offer practical guidance on how to prepare.

The SCCs were published a day after the European Data Protection Board (the "**EDPB**") published their recommendations on measures to supplement transfer tools set out in Article 46 of the GDPR to ensure that international data transfers provide an adequate level of protection to data subjects (the "**Recommendations**"). To learn more about the impact of those Recommendations on the use of SCCs and transfers more generally, see our summary of the here.



Addressing Schrems II

The new SCCs seek to address the concerns about assessing and safeguarding data transfers raised by ***Schrems II***, by introducing new obligations and strengthening existing language. One key aspect is the protocols the new SCCs include around handling public authority access requests (see ***A Helping Hand?*** below). The updates also include:

Warranties: the new SCCs include extensive mutual warranties about the local laws affecting the transfer, meaning parties must declare they have taken into account the specifics of the data transfer and the laws of the destination country. There is also a warranty to document a transfer risk assessment in all cases. This mirrors EDPB recommendations.

Security measures: the SCCs provide that any assessment of security should take account of the risks involved, the nature of the personal data and the nature, scope, context and purposes of processing. The new SCCs even refer to encryption during transmission and anonymisation or pseudonymisation. This complements the EDPB's recommendations on **technical supplementary safeguards** (see ***A Confusing Relationship?*** below).

Assessment and audits: the SCCs provide that the data exporter may look to a data importer's audit certifications when completing an audit. The exporter may also rely on an independent audit to be arranged and paid for by the importer. This compliments the EDPB's recommendations on **increasing accountability**.

In some places, the SCCs refer to the EDPB's Recommendations meaning companies will need to apply these two documents together. As such, we have set out where the SCCs incorporate the Recommendations and where there are contradictions.

A confusing relationship?

Provisions contradicting the recommendations

Assessing potential interference

Both the SCCs and the Recommendations list factors for consideration when determining whether local law allows the data importer to comply with its obligations under the SCCs. However, the factors are **different**. While the Recommendations suggest that you should not consider subjective factors (see paragraph 42), the SCCs permit you to consider *"any relevant experience"* (see *Clause 2(b)(ii)*).

Article 28

The new SCCs also purport to replace the need for the controller to impose separate contractual measures on the processor to comply with the controller's obligations under Article 28 of the GDPR where the processing involves data transfers from controllers to processors outside the EEA (see *paragraph (9) of the Implementing Decision)*.

However, the content of the SCCs are **simple in comparison** to the EDPB's guidance (published earlier this year) on controllers and processors which provides that Article 28 obligations are not sufficient in themselves and should be supplemented by detailed provisions.

A helping hand?

Provisions complementing the recommendations

In addition to the measures described above (see *the Addressing Schrems II* section), the SCCs helpfully include some other concepts recommended by the EDPB in the Recommendations. Specifically, the SCCs include the following supplementary safeguards from the Recommendations in relation to attempts by public authorities to access the exported data:

- **Immediately notify:** a notification provision requiring the data importer to notify the data exporter upon receiving a legally binding disclosure request from a public authority or upon becoming aware of any direct access by a public authority (see *Clause 3.1(a)*).
- **Request a waiver:** if local laws prohibit such notification, the SCCs also require the data importer to use its best efforts to obtain a waiver of the request (see *Clause 3.1(b)*).
- **Regularly report:** a requirement that the data importer should provide the data exporter with aggregate information on requests received at regular intervals (see *Clause 3(c)*).
- **Keep a record:** an obligation to document any request, the assessment of that request, and the response provided (see *Clause 3.1(a) & Clause 3.2(b)*).
- **Preserve documents:** data importer **must** preserve all records taken for the duration of the contract (see *Clause 3.1(e)*)
- **Always challenge:** a data importer must challenge such requests when there are grounds to do so and exhaust all available remedies (see Clause 3.2(a)).

Some practical steps

It is anticipated that the new draft SCCs will be adopted In early 2021 and companies will have one year to update their contracts with the new provisions in order to ensure their contract-based data transfers continue to be legal. Although it remains to be seen whether the UK will adopt the SCCs following the end of the Brexit transition period on 31 December 2020,, we recommend that you begin to prepare:

- ✓ **Align your documents:** you will need to check that any terms of a negotiated or template Data Protection Agreement don't conflict with the new SCCs because the SCCs include a priority clause favouring the SCCs. This is particularly relevant to liability as the new SCCs provide detailed liability provisions that are likely to conflict with their negotiated counterparts.
- ✓ **Repeal and replace:** you will need to assess your current data transfer arrangements and replace your existing network of standard contractual clauses with the new SCCs before the transition period expires in at the end of 2021.
- ✓ **Reduce your paperwork:** the new SCCs allow for multiple controllers and processers to be parties to the same set of SCCs meaning there is no need to overcomplicate data transfer arrangements anymore by requiring several SCCs for a single transfer.

Some points requiring clarification

There are some areas of the new SCCs that would benefit from some clarification before the finalised new SCCs are published. We have summarised some of the grey areas below:

- ✓ **Are controllers expected to sign processor-processor SCCs?** Requiring controllers to sign processor-processor SCCs would undermine the very decision to produce processor-processor SCC's. However, the reference to the list of parties in Annex I.A in *Clause (b)(ii)* insinuates that controllers are a party to the processor-processor SCCs.
- ✓ **Extending GDPR's extra-territorial reach:** The new SCCs require non-EEA controllers to notify the competent EEA authority of any breach likely to result in "significant adverse effects", even where they are not otherwise subject to the GDPR. This extends the GDPR's extra-territorial effect - some controllers may have to start dealing with EU supervisory authorities where they would not otherwise be obliged to do so.
- ✓ **Do processors need to identify all controllers?** The SCCs seemingly require processors to list all ultimate data controllers in Annex I.A (see *Section II, Module 3, Clause 1.1(a)*). In some instances, this would require a processor to list 100s or 1000s of controllers, which seems overly onerous.

GET IN TOUCH

Naomi Leach

Partner, data protection

T: +44 20 7809 2960
E: naomi.leach@shlegal.com

Katie Hewson

Associate, data protection

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

Olivia Fraser

Trainee solicitor, data protection

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

www.shlegal.com

STEPHENSON HARWOOD

BC1118-Standard contractual clauses-1120