European Commission's new standard contractual clauses: what they mean for UK businesses

Bridget Treacy, Hunton Andrews Kurth

This piece was originally published on Practical Law and is reproduced with the permission of the publishers.

The European Commission's long-awaited standard contractual clauses (SCCs) for international transfers of personal data made under the EU GDPR have now been finalised (see *Legal update, European Commission adopts final versions of standard contractual clauses under EU GDPR*).

SCCs are the most frequently used mechanism for transferring personal data from the EU (practically speaking, the EEA) and from the UK to third countries. They have become the default alternative for UK or EU transfers to the US, following the ECJ's decision in July 2020 to uphold SCCs (subject to case-by-case assessment of the transfer) and to strike down the EU-US Privacy Shield in *Data Protection Commissioner v. Facebook Ireland Limited*, *Maximilian Schrems (C-311/18* (the Schrems II case)) (see *Legal update, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ)*).

Key features of the new SCCs

Aside from including additional contractual provisions to address the Schrems II case, a key feature of the long awaited new SCCs is that they have been updated to reflect the requirements of the EU GDPR (the existing SCCs reflect the Data Protection Directive 95/46/EC). There are also other modifications, retained in the final version, that overall will make the new SCCs more flexible to use. These include the modular structure, recognition of processor-to-processor and processor-to-controller transfers, and a "docking" provision to enable companies to join (and leave) group arrangements for data transfers.

As before, the content of the clauses cannot be amended, but the modular structure enables the clauses to be customised, for example, provisions addressing controller to controller transfers can be omitted when the transfer at hand is a processor to processor transfer. Otherwise, the clauses convey the clear message that companies are expected to understand their data transfers in more detail than was previously the case (including onward transfers), and to document them in greater detail.

Transition and implementation

The new SCCs will take effect on 27 June 2021, and existing SCCs template will be repealed three months later, on 27 September 2021. There is therefore a three month window in which to finalise any transfer arrangements that have already been started and which will rely on the existing SCCs. If the deadline is missed, the new SCCs will need to be used.

Existing transfer arrangements that rely on SCCs will continue to be valid until 27 December 2022, provided the data processing activities are unchanged. Accordingly, there is no need to rush to implement the new SCCs. In most cases, the date by which new SCCs must be implemented is 27 December 2022, when the existing SCCs will cease to be valid.

What about personal data transfers from the UK?

Crucially, the new SCCs have not been adopted for use in the UK and the transition periods above do not apply to personal data exports from the UK, because the new SCCs were adopted under the EU GDPR. Also, this is an issue of timing: as the new SCCs have been adopted after the UK left the EU, they do not form part of retained EU law. Accordingly, UK companies cannot use the new SCCs for UK data exports, but must instead continue to use the existing SCCs. Where existing SCCs are used, the ICO has indicated that changes may be made 'so they make sense in a UK context', provided the substantive provisions of the SCCs are not changed. So, for example, changing EU Member States to the UK, and changing supervisory authorities to the ICO is permitted. The ICO has published a modified version of the existing SCCs for UK data transfers (see *ICO: Guide to the UK GDPR: Standard Contractual Clauses (SCCs) after the transition period ends*).

The ICO is preparing its own set of UK SCCs under the UK GDPR for data transfers from the UK and is expected to consult on these shortly with a view to finalising them by the end of the summer. Interestingly, ICO Deputy Commissioner, Steve Wood, said in May that the ICO is "considering the value to the UK for us to recognise transfer tools from other countries, so standard data transfer agreements, so that would include the EU's standard contractual clauses as well". It is possible that we may yet see a modified version of the new EU SCCs for use in the UK.

Schrems II requirements

When companies use SCCs as the data transfer mechanism, they must address the requirements of the Schrems II case. This is the position irrespective of whether the existing SCCs or the new SCCs are used. In practical terms, where UK companies rely on the existing SCCs they must undertake a data transfer risk assessment (step 3 of the EDPB's six steps, summarised in the *The EDPB's six steps* below), and supplement the existing SCCs with additional contractual provisions and other safeguards, as envisaged by the case itself and by the EDPB's Recommendations 01/2020 (adopted on 18 June 2021).

Where an EU exporter uses the new SCCs, they must still undertake a data transfer risk assessment, but the new SCCs contain contractual provisions that address the Schrems II case. They must still consider whether any additional contractual measures or technical or organisational safeguards are required (see Annex 2 of the EDPB Recommendations). UK companies may find it helpful to refer to the Schrems II provisions of the new SCCs as a template for any additional clauses required to supplement the existing SCCs (see *What about personal data transfers from the UK?*).

EDPB final Recommendations 01/2020 on supplementary measures

The EDPB's Recommendations clarify that controllers or processors, acting as data exporters, are responsible for verifying, on a case-by-case basis whether the law or practice of the third country importer impinges on the effectiveness of the appropriate safeguards contained in the Article 46 EU GDPR transfer tools, and if appropriate, this can be done in collaboration with the data importer. Where the data exporter assesses that the law or practice of the third

country is not "essentially equivalent" to that of the EU, they can implement supplementary measures to bring it up to the standard required.

The EDPB's Recommendations provide data exporters with six steps to follow, potential sources of information and examples of supplementary measures, to help them to comply with the requirements of the Schrems II case. The *The EDPB's six steps* are summarised in the box below (see the *Recommendations* for the full text).

The EDPB's six steps

- **Step one.** Know your transfers by mapping all transfers (including onward transfers to sub-processors) of personal data to third countries. Article 30 documentation might assist here. Verify that the data transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

- **Step two.** Verify the transfer tool that your transfer relies on. If an adequacy decision is in place, no further steps are required, other than monitoring that the adequacy remains valid. If there is no adequacy decision, then assess what Article 46 safeguard or Article 49 derogation can be relied on for the data transfer, bearing in mind that Article 49 derogations cannot become "the rule" in practice and need to be restricted to specific situations.

- **Step three.** Assess if there is anything in the law and (or) practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tool (such as SCCs or Binding Corporate Rules) relied upon, in the context of the specific transfer. Focus on the law relevant to the transfer and the transfer tool relied upon. Examine also the practices of the third country's public authorities which will help to verify if the safeguards contained in the transfer tool can ensure, in practice, the effective protection of the personal data transferred. Examining these practices will be especially relevant for the assessment where:

    - Legislation in the third country formally meeting EU standards is manifestly not applied or complied with in practice.
    - There are practices incompatible with the commitments of the transfer tool where relevant legislation in the third country is lacking.
    - The transferred data and (or) the importer fall, or might fall, within the scope of "problematic legislation" (that is to say, impinging on the transfer tool's contractual guarantee of an essentially equivalent level of data protection and not meeting EU standards on fundamental rights, necessity and proportionality). "Problematic legislation" is explained in footnote 50 of the Recommendations.

    In the first two scenarios, the data exporter must suspend the transfer or implement adequate supplementary measures in order to proceed with it. In the third scenario, in the light of uncertainties surrounding the potential application of problematic legislation to the transfer, the data exporter has a choice as to whether to:

    - Suspend the transfer.
    - Implement supplementary measures to proceed with it.
    - Proceed with the transfer without implementing supplementary measures if it is possible to demonstrate and document throughout that there is no reason to believe that relevant and problematic legislation will be interpreted and (or) applied in practice to the personal data transferred to the third country. The data exporter must do this, if necessary in collaboration with the importer, taking into account the experience of others in the same sector, and (or) other similar transfers and additional sources of information.

    For the elements to be taken into account when assessing the law of a third country dealing with access to personal data by public authorities for the purpose of surveillance,

the EDPB refers data exporters to the EDPB's *Recommendations (02/2020) on the European Essential Guarantees for surveillance measures*.

- **Step four.** Identify and adopt supplementary measures, that are necessary to bring the level of protection of the data transferred up to the standard of EU essential equivalence. This step is only necessary if the assessment reveals that the third country legislation and (or) practices impinge on the effectiveness of the Article 46 transfer tools. Annex 2 contains a non-exhaustive list of examples of supplementary measures – organizational, additional contractual measures and technical (such as encryption and pseudonymisation).

- **Step five.** Take any formal procedural steps that the adoption of supplementary measures may require.

- **Step six.** Re-evaluate at appropriate intervals the level of protection afforded to the personal data transferred to third countries and monitor if there have been or there will be any developments that may affect it.

  Assessments should be conducted with due diligence and documented, in case evidence is requested for legal reasons or regulatory investigations (see *Legal update, EDPB adopts final version of recommendations on supplementary measures for data transfers to third countries in response to Schrems II (50th Plenary)*).

Which transfers will need new SCCs?

Subject to the transition arrangements described above, organisations that are subject to the EU GDPR and engage in 'restricted transfers' (that is, they export data to a non-adequate jurisdiction outside of the EU) will be required to implement the new SCCs. This will include both EU controllers and EU processors. Businesses in the UK importing personal data under existing SCCs, will therefore be affected.

Where a transaction involves both UK and EU transfers (for example, an intra-group transfer mechanism), the contract will need to incorporate both the new SCCs (for EU transfers) and, for now, the existing SCCs for UK transfers. Where possible, organisations are likely to wait until the new UK SCCs are available before transitioning to the new EU SCCs, so that the exercise of updating their transfer mechanism is undertaken just once. That said, it is already apparent that data transfer addenda are likely to be lengthy once both EU and UK transfer mechanisms are incorporated.

Transfers to non-EEA importers subject to Article 3(2)

Unexpectedly, the *Implementing Decision* for the new SCCs notes that they may be used for transfers to non-EEA importers to the extent that the importer's processing activities do not fall within the scope of the EU GDPR. This appears to suggest that transfers to non-EEA importers that fall within the EU GDPR's extraterritorial reach under Article 3(2) are not subject to data transfer restrictions. While not stated explicitly, this would represent a significant change in the European Commission's approach. It would be consistent with previous suggestions by the ICO that transfers to entities that are subject to Article 3(2) are not 'restricted' transfers. At best, the position remains unclear. The onward transfer provisions of

the new SCCs do not reflect any change in approach by the Commission. It would therefore be prudent to await further clarification from the Commission before proactively adopting a strategy based on comments in the Implementing Decision. It is possible that the ICO might chose to clarify this point in its own UK SCCs in respect of Article 3(2) of the UK GDPR.

Conclusion

Data transfers are increasingly under the spotlight and, following the Schrems II case, it is clear that businesses are expected to address their personal data transfers in some detail. Now that the new SCCs are available in final form, affected businesses will need to make plans to adopt the new SCCs. For many, transitioning from existing SCCs to the new SCCss, and undertaking the Schrems II transfer risk assessment will be a sizeable task. Undoubtedly this task will be made more complex by the fact that there is a lag in the UK's adoption of equivalent UK SCCs. Agreements that address both EU and UK transfers look set to become lengthy documents.

To conclude on a slightly more positive note, the final EDPB Recommendations on Schrems II requirements acknowledge the role of a risk-based approach to assessing an essentially equivalent standard of data protection, and permit subjective factors to be taken into account. While the Recommendations remain somewhat conservative, these adjustments are very welcome.

And, in more good news, the European Commission is close to adopting an adequacy decision in respect of personal data transfers from the EU to the UK, before the end of the temporary bridging mechanism on 30 June, which would satisfy step 1 of the EDPB's six steps, above (see *Legal update, UK adequacy decisions agreed by EU member states: final European Commission adoption awaited*).