The New Standard Contractual Clauses: Key points to know

Data Protection Unit (DPU)

October 2021

Standard Contractual Clauses (SCCs)

This document summarizes certain key points relating to the new SCCs that were introduced by the European Commission in 2021. This document is neither legal advice nor comprehensive information. Rather, this is intended as a helpful summary, and should be read in conjunction with official guidance from the Data Protection Commission, the European Data Protection Board, and the European Commission.

What is Personal Data?

Personal data is information relating to a living individual, where that person is identified or could be identified, either directly from the information itself or when combined with other information.

Standard Contractual Clauses (SCCs)

SCCs are a mandatory requirement for the GDPR-compliant transfer of personal data to third countries.

In short, the new SCCs are intended to apply GDPR protections to personal data being sent to third countries where an "adequacy" decision has not been issued by the European Commission.

As of 27 September 2021, the old SCCs have been repealed, and so any new contracts entered into since that date must only use the new SCCs.

Existing use of the old SCCs, which may have been put in place before 27 September, will remain valid until 27 December 2022. The new SCCs must be entered into, to replace the old SCCs.

The new SCCs were introduced to provide clarity on what is required when transferring personal data to third countries. Nevertheless, the obligations on data exporters and on data importers remain onerous.

Transfer Impact Assessment (TIA) and Supplementary Measures

It is necessary, but not sufficient, for parties to agree to the SCCs. As well as the changes to the SCC clauses themselves, additional steps for compliance are required.

These include Transfer Impact Assessment, which includes considering particular aspects of the laws and practices in the third country of destination, along with:

- the nature of personal data transferred and the purpose of the processing;
- the law and practice of the third country; and
- any relevant contractual, technical or organisational supplementary measures to be implemented.

It is also necessary to consider what effective safeguards may be put in place, and to have a mechanism to ensure ongoing compliance.

DPU Contact Details

data.protection@dcu.ie

Tel:	Martin Ward	Ext. 7476
	Joan O'Connell	Ext. 6466
	Noel Prior	Ext. 8706

The below is taken from the website of RDJ Solicitors, by Sarah Slevin and Natalie Dillon

(Source: https://www.rdj.ie/insights/the-new-sccs--what-you-need-to-know):

What do I need to do?

If you are a data exporter (sending personal data controlled by you outside of the EEA) or a data importer (outside the EEA and receiving personal data on European residents) looking to rely on the New SCCs, then the following are key steps you should take.

1. **Assess your transfers**

   Review, map and document all data transfers currently being undertaken, including detail on the importing country, the processing being undertaken in that country, etc.

2. **Identify your basis for your transfers**

   If currently relying on the Prior SCCs, then it will soon be time to make a change. Consider also whether other transfer mechanisms are available – for instance, if there is an adequacy decision in respect of the third country to which the personal data is being transferred.

3. **Assess the need for these transfers**

   Consider why the data transfers you have identified need to be made. Under GDPR's mandatory principles, you must ensure that all processing, including any transfers, is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (in the case of transfers, transferred to and processed in the third country).

4. **Undertake a Transfer Impact Assessment (TIA)**

   As required by Clause 14 of the new SCCs, both parties (i.e. the data exporter and the data importer) will need to collaborate on the preparation of a comprehensive assessment on their ability to give a warranty regarding the 'laws and practices in the third country' and their impact on the parties' ability to comply with the new SCCs.

5. **Consider any possible 'supplementary measures'**

   This step is necessary if your TIA reveals that the third country legislation impinges on the effectiveness of the protections afforded to personal data in the EU. Use the Recommendations to assess what options are available to you.

6. **Decide whether to proceed with the transfer**

   It may ultimately be the case that a compliant transfer is simply not possible. In that case, it the duty of the data exporter not to proceed with the transfer. Although potentially problematic for the data exporter, it is a necessary inconvenience to ensure that the organisation does not find itself in breach of its legal obligations to protect personal data, with potential financial and reputational consequences.

7. **Keep under constant review**

   Neither laws nor transfers are static. Thus, what was previously a compliant transfer may not always remain so. For this reason, data exporters should monitor, on an ongoing basis and in collaboration with data importers where necessary, developments in laws, practices and the specific processing activities. Accountability never ceases.