Proskauer

Navigating the New Standard Contractual Clauses for International Data Transfers under the GDPR

Privacy Law Blog on **June 7, 2021**

The final version of the new standard contractual clauses ("**SCCs**") were published by the European Commission on June 4, 2021. Many organizations that transfer or receive personal data originating in the European Economic Area ("**EEA**") outside the EEA will be required to implement these SCCs with their customers, suppliers and affiliates by December 2022 to comply with the EU General Data Protection Regulation ("**GDPR**"). This is perhaps the most significant GDPR development since the passage of the GDPR. We had foreshadowed this impending development last week.

SCCs are template data transfer agreements that allow data exporters to transfer data to countries outside the EEA that the European Commission identifies as providing an "inadequate" level of data protection (including Australia, Brazil, China, India and the US). (Organizations that are subject to the GDPR cannot make such data transfers unless they use SCCs or an alternate data transfer mechanism approved under the GDPR.) The old SCCs (approved by the Commission over a decade ago) are perhaps the most popular data transfer mechanism under EU data protection law. The new SCCs, which replace the old SCCs, reflect requirements under the GDPR and the *Schrems II* decision of the EU's highest court.

What do companies need to do by December 2022?

Where SCCs are appropriate, the new form of SCCs may now be used by companies and in any event, the old SCCs must be re-papered by December 2022. This could be time-consuming and require companies to take the following steps:

1. identify which European personal data flows (including those involving employees, customers, suppliers and affiliates) will be impacted, and whether SCCs are necessary under the GDPR;

2. determine whether (and how) it is able to comply with the (rigorous) obligations under the new SCCs;
3. in response to *Schrems II*, assess – through a "transfer impact assessment" ("**TIA**") – whether (i) the laws of the country into which the data is imported (particularly, US law) is consistent with the SCCs and the GDPR, and (ii) any "supplementary measures" are necessary to boost data protections;
4. perform appropriate "transfer diligence" on customers and suppliers in connection with any data transfers;
5. identify relevant impacted contracts with customers, suppliers and affiliates; and
6. agree, where appropriate, new SCCs with customers, suppliers and affiliates and re-negotiate companion commercial agreements (including, where appropriate, any limits of liability and indemnities).

What are some of the key features of the new SCCs?

The new SCCs substantially update the old SCCs. Key features of the new SCCs include:

1. Modular – with provision for additional forms of data transfer: The updated SCCs provide for modules allowing controller-to-controller and controller-to-processor data transfers and also processor-to-controller, and processor-to-processor transfers, new forms that were not provided for under the old SCCs. These additional forms will be advantageous in complex data processing chains where the old SCCs may have been too rigid.
2. Significant focus on compatibility of laws of country of data importation: The new SCCs, reflecting *Schrems II*, require the parties to assess – via a TIA – whether the laws of the country into which data is imported will compromise data protections afforded under the SCCs (specifically with respect to the rights of governmental agencies to obtain access to such data). We consider this in more detail below.
3. Obligations regarding certain governmental data access requests: Data importers are, in certain circumstances, required to (i) notify the data exporter where it has received a data access request; (ii) assess the legal validity of such requests; and (iii) pursue legal remedies against such requests.
4. Accountability and related obligations: The new SCCs (in certain module(s)) contain provisions regarding (i) maintaining data processing records; (ii) notifying data subjects about the details of the data transfers; (iii) personal data breaches; (iv) whether/how parties may contractually limit their liability under the SCCs (including under companion commercial agreements); and (v) choice of law and dispute resolution.

5. Onward data transfers and sub-processors: Helpfully, the new SCCs (unlike the old SCCs) allow both non-EEA established controllers and process to use the SCCs for onward transfers of personal data. However, the new SCCs also impose new obligations on the parties with respect to (i) permitting onward transfers of data (in certain cases, conditioning this on data subject consent); and (ii) ensuring that such onward transfers (not merely the initial transfer) are consistent with the SCCs. The new SCCs also contain requirements regarding approvals for engaging sub-processors, which are broadly similar to the approach under Article 28 of the GDPR.
6. Data subjects as third-party beneficiaries: The new SCCs (like the old SCCs) provide that data subjects may directly enforce many of the provisions of the SCCs. This increases parties' exposure to potential privacy litigation. Data subjects are also allowed to request copies of SCCs subject to certain redactions.
7. Renewed focus on cybersecurity: The SCCs reinforce the GDPR's focus on cybersecurity. For example, Annex II requires that a detailed description of the technical and organisational measures implemented is set out for each of the modules. There are 17 suggested categories of requirements covering everything from pseudonymisation and encryption to events logging, data quality and certifications.
8. Incorporation of Article 28 GDPR provisions: The new SCCs in certain modules provide that the provisions in such modules will qualify as provisions that are required for compliance with Article 28 of the GDPR. This helpfully means that those parties will not have to separately negotiate Article 28 GDPR provisions.
9. New parties can be more easily added to SCCs: Helpfully, the new SCCs also permit new parties to accede to executed (new) SCCs more easily through a "docking" clause rather than requiring the SCCs to be re-executed every time that a new party (such as a new group company) is to be added.

What are TIAs (also known as a "Schrems privacy impact assessments")?

The updated SCCs have *Schrems II* (C-311/18) in mind. *Schrems II* requires companies that use SCCs to undertake a TIA to determine if so-called "supplementary measures" (for example, encryption) need to be put into place (in addition to those measures required by the SCCs) in light of the laws of the country of data import. Therefore, a TIA is intended to (i) assess the levels of data protection provided by both the laws of the country of data importation and under the SCC used by the parties; and (ii) in light of (i), whether "supplementary measures" are needed to ensure that the data is protected to the requisite GDPR standard.

The European Data Protection Board ("**EDPB**") has provided guidance with respect to the performance of a TIA – Recommendations 01/202 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (the "**Recommendations**"), in November 2020. However, the Recommendations have not been finalized, and the EDPB is set to issue final Recommendations shortly. A key open issue is whether the EDPB will (like the new SCCs) allow companies to take into account in connection with a TIA their own specific experiences with respect to governmental access requests (for example, whether or not the company has received such requests in the past).

Do the new SCCs apply to the UK GDPR too?

Following Brexit, the new SCCs will not automatically apply for purposes of the UK GDPR; though, of course, the new SCCs will be highly influential for purposes of UK data protection law too. The UK's data supervisory authority, the ICO, is expected to issue and consult on their own version of the SCCs in 2021.

* * * * * *

Proskauer's Privacy & Cybersecurity Practice Group is ready to assist you on your GDPR and international data transfer projects. Please contact Ryan P. Blaney, Vishnu Shankar, Kelly McMullon, Stephanie Martinier and/or Mathilde Pepin to discuss further.

View Original

Related Professionals

- **Kelly M. McMullon**
  Special International Labor, Employment & Data Protection Counsel