GDPR AND DATA TRANSFERS 2.0 - NAVIGATING THROUGH POST-SCHREMS II WATERS

Date: 10 June 2021

EU Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Noirin M. McFadden, Dr. Thomas Nietsch

Depending on whether you are an optimist or a pessimist, it will have taken the European Commission either three years and two weeks (since the entry into force of the General Data Protection Regulation (GDPR) or eleven months (since the Schrems II decision — see our Alert here) to publish its finalized revision of the most flexible tool to allow for the transfer of personal data to partners located in countries not otherwise providing an adequate level of data protection (Adequate Countries): the Standard Contractual Clauses (SCCs).

While Schrems II made headlines with its cancellation of the Privacy Shield framework, this mechanism only affected 5,000 companies in the United States. SCCs, on the other hand, remain the most widely used instrument to ensure an end-to-end sufficient level protection of personal data covered by European data protection. With their original version dating back 2001, an update was severely needed to align them with GDPR's extensive reach and requirements.

IN A NUTSHELL:

- The new SCCs were published on 4 June 2021:
  - Starting on 27 June 2021, companies will need to transition to the new SCCs;
  - On 27 December 2022, companies must have finalized their transition to the new SCCs.
- Affected companies include:
  - EU-based entities sharing data with partners and providers located in countries deemed not to offer an adequate level of protection;
  - Non EU-based entities otherwise subject to GDPR's extensive territorial reach (see our Alert here) sharing data with partners and providers located in countries deemed not to offer an adequate level of protection; and
  - Non-EU based entities receiving or processing personal data from or on behalf of EU-based partners or non-EU partners otherwise subject to GDPR.
- Key new elements include:
  - Data exporting entities will need to assess the importing countries' regulatory framework;
  - Where such framework cannot safeguard the transferred data subject to GDPR, additional measures must be implemented contractually, organizationally and/or technically;

    - Each and every step of the assessment, and the relevancy of the remediation measures, must be thoroughly documented; and
    - In the case of a controller/processor/sub-processor relationship, the new SCCs consolidate the requirements into a single agreement addressing the data processing requirements under Article 28 GDPR and the data transfer agreement.
- While the new SCCs provide for a general framework, many issues are left to:
    - The expected interpretation and guidance from the European Data Protection Board (EDPB); and
    - Contractual negotiations between the stakeholders.

MATERIAL SCOPE OF THE SCCS – FOR WHOM THE BELL TOLLS?

While the SCCs predecessors from 2004 and 2010 focused on the transfers of personal data from the European Union to third countries, GDPR's extraterritorial reach made them obsolete in several ways since 25 May 2018.

The new SCCs clarify that their scope encompasses all situations where personal data processing covered by GDPR is made available to or accessible by third parties in non-Adequate Countries.

As a reminder (see our Alert for more details), GDPR applies to the personal data processing implemented by entities that are:

- Located within the European Union/European Economic Area (EEA) and in that instance, for all the personal data processing they implement; or
- Located outside of the European Union/EEA, but for the personal data processing which would consist in:
    - Offering products or services to individuals in the European Union (e.g. localized e-commerce services); or
    - Monitoring the behavior of individuals in the European Union (e.g. cookies).

The first consequence of the SCCs will be to provide stakeholders not located in the European Union with a self-contained framework of reference to achieve their own compliance with GDPR when it applies to them.

But one aspect remains unclear at this stage: the sharing of personal data with stakeholders located in non-Adequate Countries, regardless of whether GDPR applies directly to them, would still be considered a restricted data transfer under Article 44 GDPR, as such restriction applies to the country of establishment. However, the SCCs do not address that specific situation. Hopefully, this will be clarified in the expected Guidelines from the EDPB.

Practically speaking, your company would likely require SCCs if:

- Your company is established in the European Union/EEA and:
    - Makes the personal data available to service providers (e.g. hosting service providers) located in a non-Adequate Country, especially in case of sub-contracting;

    - Shares personal data with other group companies or commercial partners in a non-Adequate Country for their own specific purposes; or
    - Provides services to entities located in a non-Adequate Country, even if your company cannot process the personal data for any other purpose than those services.
- Your company is not established in the European Union/EEA but:
    - Falls within GDPR's territorial scope and:
        - Uses service providers located in a non-Adequate Country;
        - Shares personal data with other group companies or commercial partners in a non-Adequate Country for their own specific purpose.
    - Does not fall within GDPR's scope and:
        - Uses service providers located in the European Union/EEA.

OPERATIONAL SCOPE OF THE SCCS – THE FOUR HORSEMEN

Historically, EU data protection encompassed two main scenarios for the old SCCs: (i) the data exporting entity always had to be a data controller, and (ii) the data importer could either be another data controller or a data processor.

In addition, local interpretations under the previous European Directive 95/46 sometimes exempted situations where the transfer occurred from an EU processor toward a non-EU controller. However, since the founding text was a directive, not all countries recognized such exemptions.

Finally, the old SCCs did not address onward transfers by importing data processors (sub-processing), leading to a complex contractual framework where the EU exporter would either need to directly execute the SCCs with the sub-contractor, or create an agency mechanism with the data importer.

For non-EU companies, the plurality of scenarios (as well as the plurality of versions under each scenario) led to confusion on the most relevant instruments.

The new SCCs harmonize this landscape by providing a modular template encompassing the four situations, which may now be used between:

A Data Controller Exporter and a Data Controller Importer (Module 1)

Module 1 addresses situations where each party acts as an independent data controller. The importing data controller will however be limited in the future use of the personal data for further processing. While GDPR is fairly liberal with such subsequent processing operations, the new SCCs restrict the available legal bases for these operations to only (i) the consent of the data subjects; (ii) the necessity for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or (iii) the necessity to protect the vital interests of the data subject or of another natural person. Notably absent is the necessity for compliance with a legal or regulatory obligation of the data importer where no actual proceedings have started — which can be explained by the concerns resulting from the Schrems II decision on intelligence and surveillance frameworks abroad.

A Data Controller Exporter and a Data Processor Importer (Module 2)

Module 2 will also serve the purpose of a data processing agreement mandated by Art. 28 GDPR in addition to the data transfer.

A Data Processor Exporter And A Data Processor Importer (Module 3)

This modular approach will allow companies to build their own SCCs depending on the data processing operations at stake, especially considering that these operations can be more complex than originally anticipated, often with data sharing of differing natures being extant within the same transaction.

A Data Processor Exporter and a Data Controller Importer (Module 4)

Module 3 seems incongruous in view of the data transfer aspects. While data processors subject to GDPR effectively need to address the provision of data by a controller, which may not itself be subject to GDPR, the relevant undertakings would likely take the shape of a data processing agreement characterizing the role of the processor and limiting the purposes for which it may, on behalf of the controller, process the personal data. The limited number of provisions of the draft SCCs in that scenario would tend to reinforce this analysis, as they merely address instructions, security and documentation (except where the processor combines the controller's personal data with others collected directly by the processor in the European Union).

THE TIMELINE FOR TRANSITION – FADE TO BLACK

In order to allow stakeholders to digest the new framework and proceed with renegotiations of their existing contractual arrangement, the old SCCs will remain usable until 26 September 2021, after which they will be effectively repealed and the new SCCs will become the only acceptable SCCs for new agreements.

However, old SCCs that would be in place by September will remain valid until 26 December 2022, effectively creating a 15-month transition period, provided that no change in the processing operations would require their update in the meantime.

While this may seem a lengthy window, you should not forget that the consequences of the Schrems II decision have been applicable since 16 July 2020 and the new SCCs only provides for an easier implementation of its requirements. Coupled with the many aspects of the new SCCs that will still be subject to contractual negotiations (see Section 7 below), they will therefore dictate for the transition to start without delay.

THE DETAILS OF THE PROCESSING OPERATIONS SUBJECT TO TRANSFER – NOTHING ELSE MATTERS

In line with GDPR's accountability tenets, the parties will be required to provide extensive details on the personal data processing operations associated with the transfers.

While this exercise should prove to be relatively easy where both parties performed their due diligence obligations and data mapping exercises, the overall philosophy of GDPR will also mandate that these appendices be completed as a stand-alone document.

Far too often, companies merely referr to the services provided under underlying commercial contracts to describe the processing operations at stake. Considering that the transparency tenet of GDPR will mandate that all information be provided to the inquiring data subjects or competent Supervisory Authority, and that the underlying commercial contract may not, in itself, be sufficiently clear to easily convey all requirement elements, many companies will therefore be required to populate the SCCs as a stand-alone document with all relevant details.

LIABILITY AND THIRD PARTY BENEFICIARIES... AND JUSTICE FOR ALL

Like the former SCCs' framework, the provisions of the new SCCs are in most cases expressly enforceable by data subjects, meaning they can directly claim breach of any of the parties' obligations under the SCCs in their own name and, for instance, claim remediation of such breach or compensation of damages incurred as result of such breach from the data exporter or data importer. These direct contractual claims supplement the statutory damage claims under Art. 82 GDPR which may be relevant as under certain jurisdictions contractual claims may be more beneficial for the claimant as tort law claims.

The extent of liability of the parties to the SCCs and in particular, internal allocation of liability is stipulated basically in compliance with Art. 82 GDPR, i.e., the data subject may claim damages from either data importer or data exporter but the party being subject to such claim may request compensation from the other party to the SCCs to the extent the damage was caused by that party. Consequently, limitations of liability are expected to remain a major pain point in data transfer negotiation and should be carefully reviewed.

Both data importers and data exporters must accept jurisdiction of the courts in an EU member state for any such claims brought by a data subject.

ACCOUNTABILITY AND DOCUMENTATION OF COMPLIANCE – EYE OF THE BEHOLDER

Adopting a risk-based approach, the EU Commission allows the exporter to rely on "practical experience" regarding how authorities implement access to personal data in the destination country. Therefore, it would not solely be limited by the letter of the law but also affected by its application.

This could potentially require the exporter to have legal opinions drawn by counsels in the importing jurisdiction, thereby establishing a sufficiently detailed survey of not only the legal framework applicable to the importer, but also how the framework is effectively enforced. This position seems to offer more flexibility than the EDPB's position in November, which focused exclusively on the applicable law.

Companies should therefore consider supplementing their existing data maps with a heat map of the various intelligence and surveillance laws in force in countries with which they contemplate data sharing projects. Based on this assessment, they would subsequently need to implement bespoke technical and organizational measures (TOMs) for each country, or, as a last resort, deploy the most restrictive TOMs to the whole of their operations.

Where the TOMs required for the destination countries cannot be implemented (for instance, where the data importer is a large company pressing for its data protection terms to be adopted but not sufficient in view of the assessment previously made by the data exporter), the data exporter will need to search for an alternative partner.

Further to the recent position by a German Supervisory Authority (see our alert here), the commercial onus may shift to U.S.-based service providers to come up with acceptable terms in order to continue doing business with EU companies, or any other companies that would otherwise be, legally or on a voluntary basis, subject to GDPR.

ADDITIONAL COMMERCIAL CLAUSES OR WHAT IS NOT IN THE NEW SCCS – THE UNFORGIVEN

While the new SCCs provide for a common baseline to address the international transfer of personal data, they are more a method than a contract. Indeed, while the foundational principles may be set forth in the SCCs, many critical details of implementation will remain subject to contractual negotiations.

In that regard, we notice that the draft SCCs initially provided for cost allocation for the cooperation of the data importer in establishing the data exporter's own compliance. Whether such cost allocation was fair or not, it had the benefit of leveling the playing field.

These provisions have not been enshrined in the final version of the new SCCs. It will therefore be up to the data exporter to negotiate several aspects to ensure that (i) cooperation of the data importer will not be subject to additional (and sometime prohibitive) costs, which could effectively hinder its own compliance; and (ii) service levels for such cooperation are coherent with regulatory undertakings bearing on the exporter.

These additional contractual considerations would notably include:

- How documented instructions will be conveyed from one party to the other;
- The timeline, modalities, and costs for cooperation, audit, and information requests by the other party in case of inquiries by the other party, a data subject, a Supervisory Authority, or in case of a data breach;
- The timeline, modalities, and costs for the return and deletion of the personal data held after the termination of the contract; and
- Liability aspects as detailed in Section 5 above.

However, one contractual aspect that often was a difficult point of negotiation with service providers is ultimately resolved by the new SCCs: the processor using further data processors (Sub-Processors) will need to pro-actively inform the data controller of any contemplated changes in writing. Indeed, service providers were usually relying on a webpage listing their providers, and directing the controller to regularly check such lists for any changes. This hindered controller's efforts to effectively evaluate the compliance of Sub-Processors in due time and form an objection to such appointment. Nevertheless, the process to lodge an objection will be left to the contractual negotiations. In any case, the Sub-Processors must be listed in a dedicated annex to the new SCCs, which will therefore require the parties to update the SCCs regularly.

BREXIT IMPLICATIONS – TURN THE PAGE

The United Kingdom adopted the old SCCs at the end of the transition period but due to Brexit, will not be automatically bound by the new SCCs. While it could of course choose to adopt them, the UK's Supervisory Authority (the Information Commissioner's Office, or ICO) has already announced that it will publish a new set of UK-specific SCCs for consultation this summer. Consequently, it could be several months before the UK adopts its own take on the new SCCs. This change to the EU SCCs does mean that UK and EU practice may likely diverge, and companies involved in data exports from both the UK and EU could need two sets of agreements to address each series of data flows.

In the meantime, we are also still waiting to hear if the EU will grant the adequacy decision to the UK. While a draft decision had been published, the relatively critical opinion of the EDPB on the draft UK adequacy decision published in April seem to have stalled its final adoption. As the temporary grace period granted under the Trade and Cooperation Agreement, which allowed data exports from the EU to the UK to continue will run out at the end of this month, and provided that the adequacy decision is not granted by then, UK data importers doing business with EU companies will also need to prepare for this worst-case scenario and execute the new EU SCCs.

Please join us for our webinars on 16 June 2021 for a more in-depth analysis of the new SCCs, negotiation tips and to ask all questions you would have. Click here to register.

The firm's Global Data Protection team (including in each of our European offices) remains available to assist you in achieving the compliance of your data transfers at global levels.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

NOIRIN M. MCFADDEN
STAFF LAWYER

LONDON
+44.20.7360.8135
NOIRIN.MCFADDEN@KLGATES.COM

DR. THOMAS NIETSCH
PARTNER

BERLIN
+49.30.220.029.408
THOMAS.NIETSCH@KLGATES.COM

