Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

10 December 2020

Comments by the Centre for Information Policy Leadership on the European Commission Standard Contractual Clauses between controllers and processors under Article 28 (7) GDPR

On 12 November 2020, the EU Commission issued its draft implementing decision (Decision or Commission Decision) on standard contractual clauses (SCC) between controllers and processors for the purposes of Article 28 of the General Data Protection Regulation (GDPR).[1] The EU Commission (Commission) invited public comments on this document by 10 December 2020. The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments below as input for the final Decision.

CIPL welcomes the Commission's initiative to provide SCC to assist organisations in complying with the GDPR. SCC are key to achieving the dual aim of ensuring continuity in the level of protection for personal data throughout the digital supply chain and of fostering the growth of the data economy. In addition, the SCC are instrumental in ensuring consistency of GDPR implementation across the EU and providing organisations with legal certainty. In this context, it is important that the Commission clarifies the relationship between these SCC and those adopted by the data protection authorities (DPAs) and approved by the EDPB under Article 28(8) GDPR.

Section 1 summarises CIPL's overall comments on the SCC, Sections 2 and 3 analyse some specific clauses and Section 4 provides a summary of CIPL's recommendations to the EU Commission.

1. General Comments

1.1 Align the wording of the SCC with GDPR

In several instances, the SCC wording is not fully aligned or consistent with the GDPR. To avoid any potential misinterpretation and conflicts, CIPL would recommend, to the extent possible, replicating the language of Article 28 GDPR or any other relevant Article, and not expanding the obligations or setting out stricter requirements than the GDPR. There are discrepancies, for example, with respect to the provisions on security of the processing and notification requirements in the event of a personal data breach (see below point 2.3) and appointment of sub-processors (see below point 2.5).

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Commission-Implementing-Decision-on-standard-contractual-clauses-between-controllers-and-processors-located-in-the-EU

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

1.2 Provide for more flexibility for interactions with other contracts

SCC are contractual provisions that are generally not executed in isolation, but instead in the context of a wider commercial relationship between the parties, and are therefore incorporated into commercial contracts or constitute one element of broader framework agreements.

Section I Clause 2(b) “Invariability of the Clauses” provides that wider contracts and additional clauses shall not contradict, directly or indirectly, the SCC or prejudice the fundamental rights or freedoms of data subjects. CIPL underlines that there is a tendency to follow the SCC literally and some parties may even consider that merely changing the language or format of the SCC would “contradict” the Clauses, leading to endless and counterproductive discussions. A mere re-sequencing of provisions, for example, or combination of a clause as written with a business term within a contractual paragraph does not substantively alter the protections afforded by the SCC. Some practical guidance and examples as to amendments that are permitted and those that are not would be of assistance to controllers and processors, particularly for the purposes of negotiations.

Section I Clause 4 “Hierarchy” provides that in case of conflict with an existing agreement between the parties, the SCC shall prevail. The Commission should clarify this provision is without prejudice to provisions in other existing agreements that go further than the SCC. The purpose would be to avoid reopening burdensome and lengthy negotiations with suppliers and vendors for agreements currently in place, which are already compliant with and sometimes go beyond the GDPR’s requirements. Strictly applying the SCC would require the reopening of negotiations without any benefit with regard to GDPR compliance.

1.3 The SCC should be modular

In order to address instances where a processor may provide a service to a controller in several different jurisdictions, or several services to the same controller, CIPL recommends that the SCC be provided in modular form. For example, indicating the name of the competent DPA under Clauses 8 and 9 may be impractical, especially where the one-stop-shop mechanism under the GDPR does not apply. In addition, it should be possible for the parties to sign the same SCC with several Annexes to cover multiple scenarios.

1.4 Clarify the operation of the optional docking clause

CIPL welcomes the flexibility offered by this Clause. However, some additional clarity as to how the Clause functions in practice, and how the Clause becomes enforceable from a contractual perspective, is required. For example, it appears from its drafting that accession to the SCC may occur unilaterally, with acceding entities simply executing certain Annexes. CIPL would welcome a clearer process, possibly one that requires the approval of other parties to the SCC during the accession process.

In addition, Clause 5(b) of the docking clause should be rephrased to provide that upon accession, not only does the acceding entity have the rights and obligations of the exporter or importer, but the other parties will have the relevant rights and obligations in respect of the acceding entity as well.

CIPL highlights more generally that in the event of an onward transfer to a sub-processor that agrees to be bound by the SCC, accession to SCC (if this is intended by the parties) in practice may be quite difficult as the SCC will often be incorporated into broader contracts which will not be directly binding on sub-processors.

2. Comments on the obligations of the Parties

2.1 Instructions

CIPL would welcome confirmation that instructions of the controller do not necessarily have to be listed exhaustively in Annex IV, as required by Clause 7(a), but can refer to an underlying service agreement or relevant statement of work, as more practical option in many instances. In addition, the Commission should confirm that the word "documented" includes instructions provided orally and recorded by the processor as well as instructions in writing, including through online tools. CIPL recommends also that the Commission consider that the parties may have agreed to specific formalities and procedures for the issuance of new instructions by the controller. For example, if the new instructions materially alter the parties' obligations under the underlying service agreement, they should be subject to agreed contract change control procedures.

2.2 Erasure and return of data

CIPL recommends that the Commission consider that immediate deletion or return of data may in some instances prove impractical, and some processors will require a grace period post-termination to fully purge data from their systems. For example, data is often maintained in a cloud system in which deletion occurs on a regular basis, e.g. every 30 days. In these instances the processor should be permitted to allow such processes to run their natural course, rather than being subject to an obligation to identify and purge specific sets of data. This Clause also does not make clear that the controller may request deletion or return of personal data other than at the time at which the services are terminated. The controller should be provided with the flexibility to request return or deletion at its discretion under the SCC.

In addition, it is not necessarily practical to expect the controller to select whether or not it will require return or deletion at the outset of a contract – the more practical option from the controller's perspective may only be clear at the point of termination, and therefore an option should be provided that allows the controller to make a selection at the appropriate time. In some instances, it may be most practical for the processor to share the relevant data with another processor appointed by the controller, rather than returning it to the controller. This is another option that could be added under Clause 7.2. With regard to all of these options, controllers should be provided with the ability to apply different arrangements to different data sets, for example requiring that some data be returned and some deleted.

CIPL therefore recommends including in the SCC an additional option, i.e., that, with prior notice agreed between the parties before termination of the agreement, the controller shall determine the destination of the data, which may include the deletion and/or the return to the controller and provision of the data directly to another processor appointed by the controller. The parties may also agree a default option if the controller fails to communicate its decision to the processor in the agreed time period.

2.3 Security of the processing and notification requirements in the event of a data breach

Clause 7(3)(a) should better reflect the wording of Article 32 GDPR. Article 32 states: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk." Those parts underlined above, i.e. the state of the art and the costs of implementation, are not specifically referred in Clause 7(3)(a), nor in Annex III on the technical and organisational measures, including technical and organisational measures to ensure the security of the data implemented by the data processor. If there is any reason for their removal, the Commission should make this clear. Otherwise the wording should be fully aligned with the GDPR.

Clause 7(3)(a) provides that the processor shall notify the controller without undue delay and at the latest within 48 hours after having become aware of the breach whereas Article 33(2) GDPR only requires that the processor notify the controller without undue delay after becoming aware of the breach. In addition, the processor is required to provide details such as a description of the nature of the breach, its likely consequences and the measures taken or proposed to be taken to mitigate its possible adverse effects. These are not obligations that are explicitly imposed directly on processors under the GDPR - Article 33(3) applies to breach notifications by the controller to the DPA only (Article 33(1) GDPR). It does not cover breach notifications by the processor to the controller covered by Article 33(2) as, in most cases, the relevant information may not be available to the processor. Therefore, CIPL suggests either removing the requirement to provide all details of the breach as mandated by Article 33(3) of GDPR or qualifying Clause 7.3(a) by adding "to the extent reasonably feasible taking into account the nature of the processing and the information available to the processor."

Clause 7(3)(b) and Clause 9 on the cooperation between the controller and the processor in notifying the DPA and data subjects introduces a duty to cooperate "in any way necessary" that is not mentioned in Article 28(3)(f) GDPR. As is the case with respect to processor's obligations under Clause 8, the parties should be permitted to negotiate between themselves as to the level of co-operation and assistance required, in line with GDPR provisions.

2.4 Documentation and compliance

Under Clause 7(4) CIPL recommends that negotiations on commercial decisions as to which party bears the costs of audits be left to the parties themselves. There are no requirements under the GDPR that apply to the allocation of costs with respect to audits. The same applies with respect to the notice that must be provided prior to an audit by the data controller. This is required to be "reasonable" by the SCC, but parties may wish to impose more stringent requirements from a controller perspective (for example if particularly sensitive data is being shared) or from a processor perspective (such as where a processor acts on behalf of many controllers and requires sufficient notice from each in order to prepare, or to ensure that the data of other controllers is not made available to the auditing controller). Parties may also wish to set restrictions around how often such audits may occur, or oblige the processor to permit an immediate audit in certain circumstances (such as a breach). The GDPR does not limit the ability of the parties to set out particular rules with regard to audits, and the SCC should therefore avoid doing so as well. Alternatively, CIPL recommends to make the drafting of this clause optional, i.e., enabling the parties to provide for alternative language as they see fit, including the possibility of taking into account relevant certifications[3] held by the processor or adherence to a code of conduct.

2.5 Use of sub-processors

Despite the two different options in the headings, Clause 7(6)(a) removes in practice any distinction between prior specific and general written consent to sub-processing (which are clearly provided for by Article 28(2) GDPR). CIPL recommends the review of option 2 on general written authorization since, as currently drafted, it requires the inclusion of the list of sub-processors in Annex VI which therefore becomes part of the SCC. This looks as if the exporter had consented to these organisations (Option 1), whereas, under the GDPR, it only has a right to object to the organisations chosen by the processor.

CIPL further recommends that the SCC align with the EDPB draft guidelines on the concepts of controller and processor under the GDPR, with regard to the meaning of "the same" obligations. The EDPB's draft guidelines state: "*Imposing the "same" obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same. This also means that if the processor entrusts the sub-processor with a specific part of the processing, to which some of the obligations cannot apply, such obligations should not be included "by default" in the contract with the sub-processor, as this would only generate uncertainty*."[4] CIPL recommends making clear that the same interpretation should be applied to the Commission's wording in the SCC.

CIPL notes that under Clause 7(6)(b) the processor is required to "ensure that the sub-processor complies" with the processor's obligations. This is an unachievable standard. Accordingly, CIPL recommends that the Commission consider it sufficient that the processor remains fully responsible for the performance of the actions of the sub-processor's obligations under section (d).

Further, CIPL recommends the SCC acknowledge in Clause 7(6)(c) that where a sub-processor agreement is shared with a controller, commercially sensitive information may be redacted, and the information provided limited to the information necessary to demonstrate compliance with respect to the requirement to impose data protection obligations on the sub-processor.

Finally, the SCC require that the processor notify the controller of any failure by the sub-processor to fulfil its obligations. This is not an explicit requirement of the GDPR, and should be limited to material failures that are relevant to the controller, rather than all breaches of the sub-processor agreement.

[3] This would also enable more consistency with the provisions of the standard data protection clauses for the transfer of personal data to third countries (SDPC), where Article 1(9)(c) specifically enables the data exporter to take into account the relevant certifications held by the data importer in Module 2 (controller-to-processor scenario) in deciding on a review or audit.

[4] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 Adopted on 02 September 2020 at paragraph 157.

2.6 International transfers

Clause 7(7)(a) seems to assume that international transfers under an Article 28 agreement fall solely to the processor. CIPL highlights that this may not necessarily be the case and that that in many instances the data is transferred directly to the sub-processor by the controller. The Commission should clarify how this reality is reflected under the SCC.

In addition, CIPL recommends that where the SCC cover the same issues as the standard data protection clauses for the transfer of personal data to third countries (SDPC),[5] the same language and phrasing be used to the extent possible, in order to avoid confusion, unless there is a specific rationale for the discrepancies, in which case some explanation of this rationale would be of assistance.

3. Data Subject Rights

Clause 8(a) states that processors shall notify controllers of any data subject request that is received "directly from the data subject". This ignores the rising trend of services that deliver data subject requests on behalf of data subjects. Although not all of these will necessarily constitute valid requests, CIPL suggests that any such request be referred to the controller, in order for it to determine whether or not a response or compliance is required, given that the controller is responsible for responding under the GDPR. The wording of the SCC should be updated to reflect the fact that not all data subject requests will necessarily take the same form, nor necessarily come directly from the data subject.

Parties are required by Clause 8(d) to include in Annex VII the appropriate technical and organisational measures by which a processor is expected to assist a controller. CIPL would recommend providing further guidance as to the type of content and appropriate language expected by the Commission.

4. Summary of CIPL Recommendations

- **Fully align the SCC wording with the GDPR provisions on security and data breach notification;**
- **Facilitate interactions between the SCC and other contracts;**
- **Make the SCC more modular;**
- **Clarify the practical operation of the docking clause;**
- **Clarify that instructions of the controller do not have to be exhaustively listed in Annex IV, and that parties can instead refer out to a service agreement;**
- **Clarify if "documented instructions" also covers oral instructions recorded by the processor and instructions provided via online tools;**

[5] Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

- **Allow the parties to rely on change control procedures in the event that a controller's instructions materially alter the parties' obligations;**

- **Provide more flexibility with regard to arrangements for deletion or return of personal data at the end of the service;**

- **Include "state of the art" and "costs of implementation" in Clause 7(3)(a) and Annex III;**

- **Remove prescriptive provisions from the audit clause or make the audit clause optional;**

- **Establish a clear distinction between the specific and general authorisation for sub-processing in Clause 7(6)(a);**

- **With regard to sub-processors, align with the EDPB draft guidelines on the meaning of "the same" obligations;**

- **Remove the provision in Clause 7(6)(b) that the data importer is required to "ensure that the sub-processor complies" with the data importer's obligations;**

- **Enable the processor to redact information from agreements with sub-processors to protect confidential information;**

- **Limit the obligation of the processor to notify the controller of any failure by a sub-processor to material failures that are relevant to the controller;**

- **Acknowledge that data may be transferred outside of the EU directly to the sub-processor by the controller;**

- **Update Clause 8(a) to account for cases where data subject requests are exercised by a third-party on behalf of the data subject; and**

- **Provide examples of the type of content to be included in Annex VII.**

CIPL is grateful for the opportunity to provide recommendations on the Commission's Guidelines on the concepts of controller and processor. If you would like to discuss these recommendations or require additional information, contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, or Nathalie Laneret, nlaneret@huntonAK.com.