7 August 2019

Centre for Information Policy Leadership

Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR

The European Commission (Commission) is currently working on updated standard data protection clauses for international transfers (SCC) to serve as "appropriate safeguards" that are necessary to legitimize the transfer of personal data to a third country in the absence of an adequacy decision.[1]

The Commission is currently receiving input from organisations. The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit this paper (Paper).

This Paper is intended to highlight the main challenges organisations face when relying on the existing SCC[3] and to propose practical ways to overcome these challenges when updating the clauses to the GDPR and to the reality of current business relationships and data uses.

As a preliminary comment, CIPL stresses that SCC are the most widely used mechanism by companies transferring personal data outside the EEA to comply with the obligation to provide for "appropriate safeguards" under article 46 of the GDPR. This was already the case under the EU Directive 95/46. Companies have been relying on SCC to provide a wide range of services to their clients, providers, partners and employees, including services essential to the functioning of the economy. Some of these services, in particular when they rely on cloud technology, require continuity of support services (i.e. systems development, technicians, analysts, etc.) that cannot be provided around the clock, seven days a week without access from time zones outside the EU or other countries. Equally, data flows between the EEA and countries outside the EEA are critical to the development of artificial intelligence, which requires the free flow of large amounts of data for algorithm training purposes. SCC will also most likely be the preferred mechanism for companies in a post-Brexit world to ensure continuity of existing data flows to the United Kingdom.

[1] See articles 46(1) and 46(2)(c) of the GDPR.

[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 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.

[3] EU controller to non-EU or EEA controller; decision 2001/497/EC; decision 2004/915/EC; EU controller to non-EU or EEA processor; decision 2010/87/EU. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. For the purpose of this Paper, "C to P" means Controller to Processor (2010 Template) and "C to C" means Controller to Controller (2004 Template). "FAQ 2010" refers to FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC or WP 176. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf. This document should also be updated to align with the updated SCC.

Because of the legal challenges to SCC in the Court of Justice of the European Union (CJEU), organisations have serious concerns about their ability to continue to use this mechanism going forward and the impact this may have on their business processes, business partner relationships and digital strategy. This legal uncertainty is exacerbated by the geographical limitations of the Privacy Shield (covering only transfers to the United States) as well as by the administrative burdens of the BCR approval process and their limited scope to intragroup transfers. However, this state of uncertainty should not further delay the issuing of updated SCC. The Commission should provide interim guidance to reassure the market about the validity of SCC and propose a fall-back plan in case of a decision of the CJEU impacting the validity of the new templates. This would enable a smooth transition for organisations that would minimise any disruptions to their business operations and to the effective protection of personal data upon cross-border transfer. In parallel, it is key that the Commission work with the EDPB and the supervisory authorities to facilitate and accelerate recourse to other GDPR transfer mechanisms such as certifications, codes of conduct and the use of BCR among a group of enterprises engaged in a joint economic activity.[4] In addition, separate organisations with approved BCR should be able to transfer data among themselves[5] without the additional requirement of having to rely on a transfer mechanism (which in most cases are SCC). In this case these companies will already have in place a commercial contract defining the scope of permissible data uses which will have to comply with the GDPR.

The Commission should also clarify the relationship between adequacy decisions and SCC. Organisations may be exporting data to countries that have been recognised as adequate by the Commission and still rely on SCC. There may be several reasons for this (e.g. use of SCC predating the adoption of the adequacy decision, reliance on a unique tool for all global transfers, Privacy Shield for the US requiring organisations to self-certify, or a specific request from the data exporter). In particular the Commission should explain the extent of the obligations of the parties regarding the assessment of the law of the importer and its potential compliance with SCC obligations. Where the country has been recognised as adequate, the parties should be able to rely on the assessment performed by the Commission. Conversely, the absence of an adequacy decision of the Commission should not imply that the law of the importer does not enable compliance with SCC obligations.

In addition, CIPL highlights that the current templates and their overlap with some of the wording of article 28 of the GDPR, coupled with misunderstanding of some of the GDPR's provisions, sometimes create confusion for organisations. The templates should be reviewed and updated to ensure the consistent usage of terminology. While SCC (or EU Model Clauses) have been generally used in the context of international transfers, this terminology needs to be updated. The GDPR uses the notion of "Standard Data Protection Clauses" or "SDPC" in the context of third-country transfers,[6] while SCC are mentioned in the context of processor obligations.[7] In practice, SCC are widely used as a synonym for both scenarios, which could lead to confusion.

[4] See article 47(1)(a) of the GDPR. This provision should enable the implementation of BCR processors across entities of the digital supply chain involved in similar processing operations.

[5] This case is different from transfers under the BCR processor that can only take place between entities belonging to the same group of companies and not between separate organisations.

[6] See article 46(2)(c) of the GDPR.

[7] See article 28(7) of the GDPR.

Finally, it is not always easy to determine the appropriate SCC template to be used. This situation is aggravated by the blurred definitions of the notions of controller and processor. CIPL hopes that the EDPB's current work on this issue will help to clarify the situation. The Commission should take into account this work while bearing in mind that there will always be new situations that do not fit within the existing SCC templates and that, as a consequence, any new template and guidance should also allow for a reasonable level of flexibility and adaptability to new circumstances. In sum, it is important that, in addition to releasing new, updated and flexible templates, the Commission also provides clear and simple guidance to enable organisations to better understand when SCC are required. Similarly, as the GDPR does not provide for a definition of "transfer", guidance on this matter—consolidating regulatory and case law interpretation—may be helpful.

Comments

CIPL considers it important to assess the reason for the different provisions of the SCC before drafting is undertaken. Drafting should follow policy decisions on the uses and content of the SCC.

This Paper contains the following three separate sections, each describing the practical issues, providing concrete examples and proposing solutions:

1. Structural and procedural formalities
2. Updating the substantive obligations of the SCC
3. Practical issues

1. Structural and procedural formalities

A. The issues

In any contractual arrangement there is a distinction between those points which are substantive requirements of the contract, those which are formal requirements and those concerned with the enforcement of the terms. In this section we consider the formal requirements. In CIPL's view, there is no need for the SCC to impose specific formal requirements, subject to the points made below.

The current rigid form has led to inappropriate uses of the SCC as parties attempt to artificially fit complex relationships into the rigid structure of the existing SCC, e.g. data processors styling themselves as data controllers for the purposes of overseas transfers solely for the purpose of entering into the C to P SCC with subprocessors outside the EEA. However, the form of the contract does not go to the important substantive obligations, the aim of which is to protect individual data subjects.

It should therefore be up to the parties to work out and agree on the appropriate contractual structure and procedural formalities, subject to an overriding obligation that the contract must be legally binding on the parties involved and give appropriate third-party rights.

B. Examples

The SCC should not dictate for example:

- The number of persons who can be made party to a contract;
- The role of the organisations, e.g. they could be controllers, processors or joint controllers;
- The way in which the contract is signed, e.g. it could be done by a party acting on behalf of another;
- Specific definitions, e.g. importer, exporter;
- The nature of the processing operation that can be covered by one contract;
- The choice of law clause;
- The limitation to one jurisdiction;
- The format and legal architecture of the contract (SCC could be included or appended to a commercial contract as a schedule rather than being a stand-alone contract).

Some of these points are further elaborated below:

- **SCC should not dictate the number of parties to a contract.** Currently, SCC are not adapted to multiparty situations. All SCC templates only allow for two legal entities to enter into the contract, each acting as an exporter or an importer. This does not take into account situations where there are several parties to the same agreement. The clauses rely on the assumption that data transfers are necessarily bilateral and linear. This does not align with the reality of data transfers that increasingly involve global, large-scale and complex data processing operations with multiparty, multijurisdictional and multilateral sharing of data. For instance, distributed data centres store dynamic live data with load shifts between jurisdictions (and also for fail-safe and disaster recovery) and are accessed and shared by all relevant parties. The current SCC do not enable such complexity to be captured and should be updated to reflect the reality of how data flows work, or at least made more neutral as regards dynamic data access and sharing. In addition, in the case of intragroup transfers, it is common that processing operation covers several countries, if not all the countries in which the group operates, and several group entities (sometimes more than 100) may all act as data controllers, data processors or joint controllers for the same processing operation (for instance, corporate directory, marketing, IT or HR tools). It adds little value and is overly bureaucratic to require that the exact same SCC be signed with each separate entity that requires access to the same global database. A new party may also need to adhere to the existing SCC after they have been signed, for instance where a group of companies acquire a new entity, and that entity needs to be able to use existing group applications and tools. In addition, for more legal certainly, CIPL recommends that the Commission clarifies that for an organisation to be party to an SCC, it must be a legal entity. That would bring more consistency in interpretation of the rules and prevent situations where a mere branch of a company is asked to enter into the SCC.

- **The SCC should enable flexibility in the role of organisations.** For instance, there are currently no **processor-to-processor SCC** which would allow EEA processors to transfer data lawfully to non-EEA processors and subprocessors. Such transfers are commonplace in particular in large outsourcing and cloud arrangements where the controller contracts with an EEA-based processor generally established in its own jurisdiction.[8] As a result, the controller organisation is required to

[8] A typical example would be a German service provider utilizing its India operation but the German provider contracts with the controller and receives the data-set prior to its own export. It is the EEA-based processor who will in turn transfer the data outside the EEA and acts as an exporter.

enter into a multitude of bilateral SCC with every single non-EEA entity involved in the provision of the services. Alternatively, the processor can also cover these transfers with intragroup agreements, enabling its group companies established in the EEA to enter into SCC on behalf of and for the benefit of the non-EEA entities. Additionally, the agreement between the controller and processor established in the EEA can include a mandate to the main processor established in the EEA to sign the SCC with the non-EEA-based subprocessors in the name and on behalf of the EEA-based controller. All three situations[9] create a great deal of administrative work for all parties, in addition to being artificial and inconsistent with the commercial structure and the contractual liability rules. They are also impractical when working with large multinational service providers who use hundreds of subprocessors across numerous jurisdictions. In relation to **controller-to-controller SCC covering joint-controller situations**,[10] having a "one-size-fits-all" template would be challenging, as this situation is, by nature, contextual. Therefore the allocation of tasks and liability to each party cannot be predetermined. A template could only predefine the items that each party would need to address on a case-by-case basis regarding the allocation of tasks and, thus, liability.

- **The SCC should not specify the nature of the processing operation that can be covered by one contract.** In most cases, controllers and processors use, buy, subprocess and procure tools and services that contain a wide array of processing activities as opposed to just a single processing operation with a single purpose. Since the SCC have to be signed and appendix 1 needs to be filled out for each specific processing operation that is defined according to its purpose, with no possibility to modify the SCC, this leads to companies' having to sign a huge number of similar SCC with just appendix 1 differing, which brings no real added value. Controllers and processors should not be required to sign SCC for each and every processing operation when it is part of the same broader processing. For example, a processor receives personal data from a controller to deliver the service as part of the main contract on the instructions of the controller, but such processor may also be processing additional personal data for its own purposes as a data controller, for instance for fraud prevention or security purposes in the context of delivering the services to its client.

- **The SCC clauses could be included or appended to a commercial contract as a schedule rather than being a stand-alone contract.** Since they are not modifiable, SCC are not flexible enough to apply to a variety of situations. They often need to be better integrated into the broader complex business processes and contractual relationship of the parties. As per recital 109 of the GDPR, the parties are permitted to add new provisions to the SCC to cover business-related issues (provided that these do not contradict the existing SCC). As it stands, it is not entirely clear what type of change would constitute a contradiction to the SCC.[11] Any change that constitutes a contradiction is only valid with the prior approval of the relevant supervisory authority, which will likely cause delays to getting the relevant terms in place.

[9] See question 3 of the FAQ on pages 4 and 5.

[10] CIPL wishes to underline that a controller-to-controller transfer does not necessarily cover a joint controllership situation.

[11] See example related to audit in chapter III.B page 10.

- **The SCC should not mandate the choice of law clause or be limited to one jurisdiction.** The current SCC mandate that they be governed by the law of the Member State in which the data exporter is established. As many international organisations have complex corporate structures, there are instances in which the ultimate controller is a company that is incorporated in a non-EEA country.

C. Recommendations

The Commission should work with a small group of advisers who are familiar with the SCC to agree which points of the SCC cover substantive obligations and which cover structural and procedural formalities. A clear distinction should be drawn between the two types of provisions. Once the categories are agreed it should be made clear that parties may structure the formal parts of the contract as they wish, although possibly some guidance on the structural formalities could be prepared to accompany the substantive clauses and suggest precedents that could be used.

It should be clear that the formalities must operate so as to meet the required standards of legal clarity, certainty and effectiveness, but within those parameters users should be able to agree on the structural and formal arrangements that work for them.

The requirements would be self-policing in that it is in both parties' interests to ensure that a valid and binding contract is in place to safeguard transfers. As an additional safeguard, supervisory authorities could require as part of an audit access to all SCC used by controllers and processors.

Guidance on the structural formalities should provide for several options and include, for instance, the following:

- **The SCC should expressly enable signing by multiple parties or on behalf of multiple parties** in cases where the data must be transferred to multiple companies.

- **The adherence/accession of one party to respect all terms of an existing SCC** should be possible in a simple manner (subject to the national provisions on contract laws).

- **The SCC should be made applicable by reference in the main contract.** This would align with current market practices.

- **To address issues relating to defining governing law, dispute resolution and jurisdiction clauses,** the new SCC should not limit the applicable jurisdiction to that of the data exporter but allow for any jurisdiction on which the parties agree. In case of multiparty agreements, the SCC should be more flexible and be defined on a case-by-case basis. In particular, article 9 of the C to P SCC should not require the parties to provide for an applicable law "ex-ante" but could enable them to provide, for instance, that the applicable law shall be that of the data controller.

- **The Commission should consider the processor-to-processor relationships** by delinking respectively the notions of exporter and controller on the one hand and the notions of importer and processor on the other hand. The SCC should enable a processor to act as an exporter and transfer personal data to another processor outside the EEA. The processor exporting personal data outside the EEA would not be acting as an agent of the controller but would be acting as an independent entity subject to its obligations under the GDPR. This would be consistent with commercial relationships in general and would provide the required flexibility to address specific situations while simplifying the process and reducing the creation of time-consuming, expensive and artificial contractual links.

- **The same SCC should be able to cover all processing relating to the same** contractual relationship to adapt to sector- and technology-specific cases, for instance in multicloud service environments or IoT or AI projects. To do so the parties should have flexibility to add additional appendices to the SCC and organise them in accordance with the processing operations.[12]

- **The SCC should allow organisations to use alternative language** as long as a firm set of principles is complied with (to be listed in a principle-based manner consistent with article 28 GDPR, with possible alternative language and examples). This would also enable organisations to insert these principles in a broader commercial contract without the explicit need to have a separate set of clauses. Changes to the SCC would be possible within specified parameters while avoiding the burden of seeking supervisory authority approval (which in most cases is not practical or possible). It is only in case of changes to the SCC outside the specified parameters that authorization from the supervisory authority as per article 43(3)(a) would be required. As an alternative solution, the standard SCC language could be kept to a strict minimum to cover only transfer-related obligations and leave the parties with flexibility to negotiate article 28–related provisions. Finally, the Commission could also specify which clauses of the SCC can be varied (to provide a degree of flexibility) and provide some examples of acceptable or unacceptable variations.

2. Updating the substantive obligations of the SCC

A. The issues

There are a number of updating points to ensure that the SCC are consistent with the GDPR that need attention. The updating points should also take into consideration an assessment of the SCC obligations in light of the current business models and relationships as well as modern use of data that have evolved substantially.

These updating points focus on the substantive obligations under the contracts, although in some cases the issues intersect with practical points, or raise questions of interpretation, so interpretative and policy choices will need to be made in respect of those. It is important that such policy and interpretative points are considered clearly before drafting decisions are made.

The guiding policy considerations should be to ensure the SCC protect the rights of individuals and provide legal certainty.

[12] There could be, for instance, one appendix per processing activity including the relevant security measures. Alternatively, there could also be one appendix describing all processing operations and one appendix describing security measures. The parties would remain free to decide how to proceed.

B. Examples

The following are the most relevant examples of the updating issues:

- **The broad territorial scope of the GDPR should be considered**. This involves considering whether an organisation in the EEA that transfers data to an organisation outside the EEA that is caught by the extraterritorial provisions is treated as making a transfer.[13] In this particular case, the question is whether this requires SCC or any other adequate safeguard when the non-EEA recipient is already subject to GDPR by virtue of article 3(2) (i) irrespective of the transfer at hand; or (ii) due precisely to the transfer at hand (and therefore, only limited to the data and purposes specific to this transfer). Similarly, this requires considering whether an organisation outside the EEA which is subject to the GDPR by virtue of article 3(2) is making a transfer covered by the GDPR if it transfers data to another organisation in the same country or in another non-EEA country.[14] Finally, the broad territorial scope of the GDPR may also have the effect of subjecting the SCC to a law that is not that of a Member State of the EEA.[15]

- **The relationship of the SCC with article 28 contract should be clarified**. Where a controller works with a non-EEA processor or an EEA processor works with a non-EEA subprocessor, the requirements of both the SCC and article 28 GDPR must be met. Certain provisions of the current SCC are redundant[16] or even in conflict[17] with article 28 of the GDPR. The options are to provide clauses for C to P contracts that would incorporate article 28 requirements, or to make it optional for the parties as to whether the article 28 requirements are included in the SCC or incorporated into the commercial clauses. As a general recommendation, if SCC are kept separate, they should not address issues of a purely commercial nature, such as indemnification and liability.

- **It should be considered whether the SCC should incorporate other GDPR obligations** such as accountability or breach notice by data processors (including obligation to assist the controller) or confidentiality obligation.

- **The position of data subjects and their rights** to take legal action against controllers or processors engaged in processing should be considered, in particular whether this removes the need for the SCC to engage third-party rights as standard because of the effect of article 79 of the GDPR. Possibly such a clause should only be required where the receiving controller or processor is not subject to GDPR by virtue of article 3(1) or 3(2) of the GDPR.

[13] As noted, this intersects with the question of formalities and parties.

[14] For example, a US, Peruvian or Australian company may be caught by the GDPR because it offers services to EU citizens, and wants to transfer their data from their own country to another non-EEA country, i.e. Brazil (provided of course that such organisation is not itself separately subject to the GDPR by virtue of article 3(2)).

[15] See article 9 of the C to P SCC which provides that the clauses shall be governed by the law of the Member State where the data exporter is established. When the exporter is not established in the EEA and is subject to the GDPR by virtue of article 3(2), the SCC will be governed by the law of a state that is not in the EEA.

[16] See article 5 (f) of the clause on audit rights and article 28(3) of the GDPR.

[17] For example, article 28 GDPR requires that on termination of the services, the processor must delete/return the data unless EU or Member State law requires ongoing storage. However, clause 12 of the C to P SCC, while addressing the same point, just refers to any legislation imposed on a data importer, rather than specifically referring to EU or Member State law.

- **The obligation which requires the data importer to agree that it has "no reason to believe" that the laws applicable to it prevent it from fulfilling its SCC obligations**[18] in connection with data subjects' third-party beneficiary rights[19] may be very challenging to comply with in practice. This would mean that a data subject could be claiming against the data exporter for the data importer's failure to hold a reasonable belief that it could comply with both its local laws and the obligations of the SCC and the instructions of the exporter. It is unclear how the data exporter would defend against this claim and whether it would even be possible for the data subject to successfully secure compensation if the obligation is breached. All parties have a mutual interest in ensuring that the SCC obligations are enforceable to engender trust in the framework and personal data processing more generally. This obligation currently undermines that trust by imposing a standard that companies cannot meet and providing data subjects with a level of assurance that is not achievable or potentially even enforceable.

C. Recommendations

The Commission should work with a small group of advisers[20] who are familiar with the SCC to consider how substantive provisions of the SCC should reflect the GDPR provisions and current business relationships and produce a table of recommendations. CIPL recommends that the Commission work closely on this matter with the EDPB,[21] which is currently finalizing its guidelines on the territorial scope of the GDPR,[22] and that it consider providing practical guidance to clarify the specific circumstances in which SCC have to be signed.

It should also be considered whether the SCC should make inclusion of some GDPR provisions optional or permit parties to incorporate the provisions directly into the commercial terms of the contract. The question as to whether SCC could serve as a data processing agreement, if relevant to the particular situation, should also be considered.

Finally, in relation to the third-party beneficiary clause, it may be relevant to narrow the list of the clauses of the SCC that the data subjects could enforce against the parties to limit it to situations where the data subject can actually secure compensation under local law if the obligation is breached.

[18] See Clause 5 (b) of the C to P SCC.

[19] See Clause 3(1) of the C to P SCC.

[20] CIPL would be willing to be part of this group. If deemed necessary by the European Commission, CIPL could also provide a table of proposed updates to the SCC substantive obligations.

[21] In relation in particular to processor-to-processor SCC, the WP 29 issued a working document 01/2014 on draft ad hoc contractual clauses "EU data processor to non-EU sub-processor". CIPL suggests that the Commission reach out to the EDPB to review the comments submitted by industry in this context.

[22] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en and CIPL's response: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_edpbs_territorial_scope_guidelines.pdf.

3. Practical issues

A. The issues

A number of practical issues need to be considered, in particular, the question of how all the SCC currently in operation should be handled.

SCC have been the mainstay of transfer arrangements for many years so there is a significant volume of SCC in place across the EEA. In most cases of C to P contracts the parties will already have been through one process to amend the commercial terms to comply with the GDPR requirements.

There has never been a P to P contract approved and that has proved to be a practical problem for many transfers.

The introduction of the one-stop-shop arrangements raises new practical challenges as the lead authority will be responsible for supervising all SCC for controllers and processors that are subject to their supervision.

B. Examples

The following are examples of practical issues:

- **Keeping SCC up to date**. SCC are legal document that may take up to six months to be signed between the parties. The appendices are quite prescriptive and often give rise to intense discussions between the parties. In the event of any change in the processing, in the categories of data, the recipient, supplier or country, the processing operation or in the applicable technical and organisational measures, the parties are required to sign an amendment to the SCC to reflect the new situation. This contractual update can be burdensome, time-consuming and expensive, for little practical benefit. Given the number of processing operations in certain companies, it can be very challenging to keep SCC up to date with the reality of processing operations and technological changes.

- **Dealing with existing SCC**. Some organisations may have to enter into a large number of SCC both on the provider side when they procure services entailing the transfer of their clients' or employees' personal data to third-party providers (IT and security solutions, travel agency, marketing services, etc.) as well as on the client side when they sell services entailing the processing of personal data. In some organisations, the number of signed SCC rise above 100, 1000 or even 10,000. Having to update all existing SCC signed under the current templates to migrate them to a new template would require an enormous amount of administrative work from organisations that may have recently updated their current contracts to reflect the provisions of GDPR. The practical difficulties and expenses, if not the impossibility, of having all these contracts up to date within a quick time frame should be acknowledged by the Commission and the supervisory authorities.

- **Dealing with audit rights in contracts**. In many cases it is impractical for processors to allow controllers to audit their processing in view of (i) the significant administrative burden (service providers cannot allow all their customers to have an on-premise audit right) and (ii) the security issues arising from this obligation. One of the options is for the processor to have the audit performed by a third party with the adoption of an audit report. Data importers frequently attempt to amend the audit provisions in clause 5(f) of the SCC, to adapt the right of the data exporter to conduct a full audit of the data importer's facilities, sometimes in line with the suggestions of WP29 opinion regarding cloud services[23] (e.g. independent annual external audit according to a specific security standard, such as some ISO standards). As this issue is not specific to cloud services providers, and this is a variation of the existing SCC endorsed by the WP29 and not the Commission, it is unclear as to whether this amendment should be deemed acceptable per se or would need to be formally approved by the relevant supervisory authority.

- **The descriptions of the processing operations** can be problematic as it is unclear how specific the descriptions should be. One option would be the possibility for the parties to follow the article 30 record-keeping structure for the description if appropriate.[24] Another option would be to align with the provisions of article 28.3.

- **Inserting SCC into the digital supply chain:** C to P SCC are drafted on the premise that a controller contracts the whole or part of its processing to a processor, but the reality is much more complex: subprocessing operations have become a standard service with all features predefined by the processor and offered to controllers for all or many different portions of their processing activities (for instance, cloud computing, IT, maintenance, storing, cyber risk management, etc.). The notion of processing in the law has a very broad definition, encompassing at the same time situations where: (1) the processor is acting on precise instructions of the controller for processing operations that the controller has outsourced and (2) the processor is proposing a standard service to the controller to optimise its IT or processing capabilities. In the latter case, the processor offers a packaged service to the controller with existing subprocessors that are part of a digital supply chain with contractual agreements already negotiated and signed before anything is discussed, negotiated or signed with the end-customer (the controller). In practice, the importer is faced with two main challenges. First, the current SCC requires the importer to obtain the prior written consent of the data exporter each time it wishes to engage a subprocessor, which is not practically workable in particular in case (2). Second, the 2010 FAQ has led controllers to request that SCC be entered into directly with the subprocessors[25] of the importer. This leads to subprocessors having to sign potentially an uncontrollable and unforeseeable number of SCC with controllers (i.e. the customers of their customers) which are entities with which they have no existing direct commercial relationship. This triggers obligations and liabilities for which corresponding risk has not been factored into the contract, and for which proper provisions have not been made. This creates long discussions, negotiations and misunderstandings in the supply

[23] Opinion 05/2012 on Cloud Computing https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[24] This should not mean an obligation to reproduce the exporter's inventory "as is" because the transfer should not necessarily cover all the data and purposes of the original inventory entry or contain the same level of granularity and the same security measures.

[25] See question 3(a) page 4 of 2010 FAQ.

chain. Finally, the current C to P clauses do not enable a data importer, who transfers data to a subprocessor which in turn provides services to such data importer for several data exporters, to make use of a single set of SCC executed between the data importer and the subprocessor on behalf of all these data exporters. The importer has to enter into SCC on behalf of each exporter with the non-EEA subprocessor. Being able to rely on one set of SCC for all customers would be particularly helpful for public cloud services which mostly rely on standard policies and practices which are substantially the same for all data exporters that use these services. This would result in a lighter administrative burden for data exporters, data importers and the digital supply chain as a whole.

C. Recommendations

- **The Commission should provide for a grandfather clause** enabling the current contracts to remain valid under the GDPR or, at minimum, enable organisations to prioritise the uptake of the new SCC template on the basis of the following criteria:[26]

  (1) When the main contract has already been updated to the GDPR and in particular in C to P relationships, and when article 28 provisions of the GDPR have already been signed by the non-EEA entity, the update of the SCC to the new template should not be a priority;

  (2) More generally and in line with the risk-based approach of the GDPR, organisations should be enabled to prioritise the update of the SCC on the basis of potential risk of the processing to individuals.[27]

- **CIPL recommends that the updated version of the SCC is aligned with the wording of article 30 GDPR** to facilitate the filling-out of the appendices.[28] As an alternative solution to streamline the process, CIPL recommends that the appendices be replaced by a reference to the relevant category of the article 30 record of processing of the controller. Such category of the record of processing should be shared with the processor and confirmed in writing (including by electronic means[29]). This should be deemed as an acceptable agreement between the parties fulfilling the conditions of article 46(2)(c) of the GDPR. Of course, this does not prevent the parties entering into a more formal contractual amendment should they wish to do so. In case of an audit from the supervisory authorities, the presentation of the signed SCC together with the record of processing approved by the processor should be deemed sufficient evidence of an update of the SCC.

- **In line with article 28 of the GDPR, importers must be permitted to engage subprocessors under a general authorisation of the exporter**. This aligns with the requirement for external

[26] Of course, new commercial and contractual relationships entered into after the new template SCC has been released should use it.

[27] For instance, processing operations subject to a DPIA should be updated as a matter of priority.

[28] Under article 30 of the GDPR, the controller and the processor are under the obligation to maintain a record of processing containing the main features of the processing. It is worth noting the categories of information that need to be recorded in appendix 1 of the C to P SCC almost align with the wording of article 30.1 of the GDPR.

[29] See article 30.3 of the GDPR which provides that the records shall be in writing, including in an electronic form.

subprocessing under the BCR[30] that provides that subprocessing by a nonmember of the BCRs is permitted only with the prior informed specific or general written authorisation of the controller. This also better reflects the operational reality of personal data processing in complex value chains where obtaining consent from all companies is very difficult if not impossible.

- **Importers should be enabled to enter into one single set of SCC in a P to P relationship when they are processing personal data and acting on behalf of different controllers**. Such controllers could be granted third-party beneficiary rights.

- **The Commission should consider guidance to identify the security standards** that are acceptable and address how this list would be updated if new standards are deemed appropriate in the future, without the need to re-execute the SCC.

- **With respect to audits,** the Commission should also provide that it is an acceptable modification of the SCC for providers to mandate an accredited third party to conduct a regular audit of their data processing facilities and provide the certificate to the data exporter and supervisory authorities on request.

Finally, CIPL would suggest that the Commission improve the format of the SCC to propose one single electronic template with a drop-down menu covering possible situations (C to P, C to C, P to P, multiparty processing, multiprocessing, etc.) that organisations can choose from and that will generate a bespoke template specific to their situation. The Commission should also receive feedback from organisations in real time so as to update the template to take into account new cases. The 2010 FAQ should also be updated and provided in a more user-friendly and open manner, such as for instance an electronic FAQ updated in real time to address new questions and issues submitted by organisations.

Conclusion

CIPL is grateful for the opportunity to provide comments to assist the Commission in updating the SCC. If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Sam Grogan, sgrogan@huntonAK.com.

[30] Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules page 18. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.