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 for the Transfer of Personal Data to Third Countries Pursuant to the GDPR

On 12 November 2020, the EU Commission issued its draft implementing decision (Decision or Commission Decision) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation 2016/619 (New SCC).[1] The EU 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 EU Commission's update of the SCC to align them with the GDPR taking into account the Court of Justice of the European Union's (CJEU) 16 July 2020 "*Schrems II*" decision (Court Decision).[3] The New SCC are an essential step towards improving legal certainty in the aftermath of the Court Decision which upheld the validity of the SCC. As expressly mentioned by Recital 101 GDPR, flows of personal data to and from countries outside the Union are necessary for international trade and international cooperation. In this context, it is essential that the New SCC offers a practical tool to enable organisations to continue to transfer data outside of the EU while maintaining the high level of protection under EU law, especially in view of the current uncertainty on the use of other GDPR transfer tools.

CIPL welcomes the EU Commission's pragmatism that accounts for the complexity and speed of modern processing chains by shifting to a modular and multi-party approach. In addition, the New SCC fill a legal vacuum for processor-to-processor transfer scenarios and enable better accommodation of the realities of the digital supply chain. CIPL also appreciates the New SCC's dual function of providing an international transfer tool and enabling organisations to meet the requirements of Articles 28(3) and (4) of the GDPR,

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

[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.

[3] The CJEU confirmed that SCC are a valid mechanism for the transfer of personal data outside of the EU, while invalidating the EU Commission's adequacy decision on the EU-US Privacy Shield, considering that US law does not provide essentially equivalent protection for fundamental rights to data protection. It also held that in the absence of an adequacy decision by the EU Commission, organisations relying on SCC for data transfers should assess the laws of the recipient country on a case-by-case basis, in order to verify the effectiveness of SCC in ensuring compliance with EU data protection requirements. Where SCC would not be fully effective, organisations need to consider additional safeguards and supplemental measures to the protection offered by the SCC. The Court's judgment also requires DPAs to use their statutory powers to suspend or prohibit a transfer based on SCC if, in light of all the circumstances of that transfer, it considers that SCC cannot be complied with and the protection of the transferred data cannot be ensured by other means. *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, 16 July 2020, Case C-311/18, http://curia.europa.eu/juris/liste.jsf?num=C-311/18.

thereby reducing unnecessary and cumulative administrative work to sign agreements with duplicative clauses.[4]

CIPL also welcomes the EU Commission's efforts in adopting a workable solution that takes into account the reality of business relationships by (1) providing for the possibility of including SCC in a broader contract and avoiding the administrative burden of having multiple signature pages and a multiplicity of contracts; (2) acknowledging the need to preserve confidential business information by permitting companies to redact the SCC and provide a meaningful summary of their clauses to the data subjects; and (3) explicitly allowing exporters to take account of relevant certifications of the importer and of an independent audit mandated by the importer.

Finally, CIPL fully supports the EU Commission's holistic risk-based approach to international transfers that enables organisations to factor all the specific circumstances of the transfer into the risk assessment, including past history of government access requests, as reflected in Clause 2(b) and in Recital 20 of the Commission Decision.[5] This is consistent with the GDPR and the Court Decision which both require companies to assess tangible risks to data subjects, including their likelihood and severity, and not theoretical or remote risks.

More generally, CIPL would encourage the EU Commission to take further account of the fact that SCC are used in the context of a broader commercial relationship and should, therefore, seek to be outcome-focused, concentrating on achieving certain outcomes rather than complying with prescribed requirements, as much as possible.

Additionally, the New SCC should seek to achieve the dual aim of assuring the level of protection of personal data outside of the EU while also fostering the building of the emerging data economy. In their draft form, some provisions of the New SCC may result in overly burdensome processes for companies while creating unrealistic expectations. Only a few multinational companies would be properly resourced to implement certain of the proposed new requirements, thereby creating a significant disadvantage for SMEs.

Making compliance too burdensome for EU organisations may also discourage non-EU organisations from engaging in business relationships in the EU. This may be because of the prohibitive cost of implementation of the SCC for the importer even in low risk situations together with enhanced compliance risks that may lead non-EU organisations to prioritizing cooperation with partners from other jurisdictions and, therefore, putting European companies at a competitive disadvantage.

[4] CIPL White Paper on Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR (August 2019).

[5] See CIPL's White Paper on A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf.

1. General comments on the New SCC

1.1 Clarify the scope of application and scenarios covered by the New SCC

CIPL welcomes the clarification that the New SCC should also cover data transfers from a controller or a processor subject to GDPR to a controller or processor not subject to GDPR.[6] This also confirms that Chapter V GDPR does not apply to the collection of data directly from individuals in the EU, but only covers subsequent transfers of data between organisations within (exporters) and without (importers) the scope of the GDPR. This clarification is very welcome especially as several UK based organisations will be facing this situation post-Brexit.

CIPL continues to question the relevance of adding the EU Processor to the non-EU Controller scenario (P to C - Module 4). This scenario is confusing and looks irrelevant in practice, especially since Module 4 would apply only if the EU processor combines the controller's non-EU data with EU data collected by the processor. In this specific case, the EU processor could either (1) be a controller with respect to that specific data collected in the EU and Module 1 (controller-to-controller or C-to-C) would apply to the transfers to the non-EU controller or (2) be acting on the instructions of the non-EU controller which would be subject to the obligations of GDPR already as far as these instructions relate to the processing of EU data, in which case no transfer outside of the EU would take place. More generally, CIPL believes that forcing these clauses on EU-based data processors offering services to non-EU controllers which do not even target the EU market would have the effect of placing EU-based processors at a distinct competitive disadvantage by the imposition of bureaucratic compliance requirements and ineffective restrictions which the controller is not bound by or itself required to undertake and which would not be enforceable.[7] In addition, this Module tends to undermine the C to P relationship, by giving an important level of discretion and authority to the processor. This may be particularly problematic for importing controllers who are themselves directly subject to a regulatory regime which includes the controller/processor distinction such as the UK GDPR or the Brazilian LGPD. If the Commission ultimately decides to keep this Module 4, CIPL strongly recommends that it provide concrete use cases and guidance to enable organisations to understand the scenarios it covers and the interplay with the modules of the SCC.

In addition, to ensure maximum flexibility, the Commission should clarify that the multi-party approach is intended to work horizontally (e.g., one controller to many processors) and vertically (e.g., controller, processor, sub-processor), or both. For instance, this would allow the controller to be a party to the SCC in Module 3.

Finally, CIPL understands that the "legal data flows" (i.e., based on the legal relationship between the parties) only should govern the application of the relevant SCC scenario to the exclusion of "factual data flows" (i.e., based on actual physical data flows). For instance, in case a non-EU sub-processor factually accesses the data directly from the EU controller, this should not require them to enter into SCC as long as the relevant SCC and onward agreements are in place respectively (1) between the exporting controller

[6] See Clause 1(b)(i) and Recital 7 of the Commission Decision.
[7] See CIPL Comments on the EPDB's Territorial Scope Guidelines, 18 January 2019, analysing the scenario where non-EU personal data is sent back by the EU processor to the non-EU controller and demonstrating that subjecting this scenario to Chapter V GDPR would be irrelevant and counterproductive.

and the importing processor and (2) between the importing processor and the sub-processor, even if the data does not pass through the importing processor.

Summary of CIPL recommendations:

- **Remove Module 4 from the SCC or alternatively provide concrete use cases and guidance to organisations to clarify the scenarios covered and the interplay with other SCC modules;**
- **Clarify that for maximum flexibility, the multi-party approach is intended to work horizontally and vertically; and**
- **Confirm that the legal data flows (and not the factual data flows) trigger the application of the SCC.**

1.2 Align further the New SCC with the GDPR accountability and risk-based approach

It is of the utmost importance that the New SCC integrate and reflect fully the GDPR risk-based approach that relies on an assessment of the impact of the processing on individuals, i.e., assessment of the likelihood and severity of harm to individuals in a context-specific way. CIPL recommends that the New SCC make an explicit reference to the accountability principle and the risk-based approach of the GDPR to help with SCC interpretation when they are used in commercial relationships or are interpreted by DPAs or courts in the context of enforcement.

The Commission has proposed a novel requirement that organizations "warrant" conditions in third countries that is not expected of them in the context of transfers authorised under any other provision of the GDPR. For example, where transfers are permissible on the basis of an Article 45 adequacy finding to New Zealand, organizations are still expected to conduct risk-based assessments with respect to the nature and content of the transfers, but are not required to provide any warranty thereupon. More generally, the Commission Decision should acknowledge the impossibility for organisations to warrant a zero-risk environment surrounding the transfer of personal data - especially on the basis of factors that are beyond their control - and refer to the room to maneuver left for organisations to make business decisions on the basis of these risk assessments. It is generally impossible for an organisation to warrant that an event will or will not occur when it has no direct control over it (such as a fire, flood, cyberattack or law enforcement request). The organisation can only commit to using reasonable efforts to avoid it and to mitigate the effect of such an event should it occur. A better approach is the approach embedded in Article 32 GDPR on the security of the processing that only imposes an obligation on the controller and the processor to take measures appropriate to the risk and does not require them to warrant that a data breach will never happen. Therefore, replacing a warranty requirement with the risk-based language of the GDPR would introduce better alignment and harmony with other provisions in the law. Alternatively, CIPL suggests that any obligation on the parties to provide warranties is always tempered by a qualifier such as "on the basis of the risk assessment performed by the organisation and the available information."

Summary of CIPL recommendations:

- **Make an explicit reference in the SCC to the accountability principle and the risk-based approach of the GDPR; and**
- **Replace the warranty obligation with an obligation to take measures appropriate to the risk or, alternatively, temper the warranty obligation by a qualifier that the warranty is provided "on the basis of the risk assessment performed by the organisation and the available information."**

1.3 Take into account organisations' existing GDPR compliance work

While CIPL welcomes the New SCC also covering the requirements of Article 28 GDPR in C to P and P to P scenarios, CIPL suggests that these provisions remain optional. CIPL understands the inclusion of Article 28 provisions to be more practical, especially for SMEs, but underlines that mature organisations may have already invested substantial time and resources for compliance with Article 28 GDPR. Adding these provisions again in the New SCC as mandatory wording may not be adapted to all C to P situations and may add a lot of confusion, duplication and questions from their business partners that would delay their implementation. At the same time, CIPL understands that the New SCC may also be a possible means that organisations choose to implement Article 28 in practice.

In addition, CIPL highlights that organisations have been working extensively to build relevant internal frameworks and tools for data protection risk assessments. Organisations are currently integrating the requirements of the Court Decision to assess transfers into these existing processes. The New SCC should not be construed as creating separate/isolated documentation requirements but should rather enable the risk assessments to be part of these existing frameworks and to be performed according to the categories of transfers, sector or data categories. Organisations should also be able to leverage the measures, tools and processes in place to comply with GDPR accountability requirements, such as for instance records of processing activities, assessment whether a DPIA is required or overall vendor due diligence.

Summary of CIPL recommendations:

- **Make the inclusion of Article 28 GDPR provisions in the SCC optional; and**
- **Enable organisations to leverage their existing GDPR compliance efforts so that SCC are not construed as creating separation and additional requirements.**

1.4 Align the wording of the New SCC with GDPR

In several instances, the New SCC wording is not fully aligned or consistent with the wording of the GDPR. This is the case, for instance, with respect to:

- Transparency obligations in Module 1;
- Storage limitation and erasure or return of personal data in Module 2;
- Security of processing in Modules 1, 2 and 3;

- Answer to data subject rights and management of unfounded requests in Module 1;
- Obligation for processors to verify accuracy of data in Modules 2 and 3; or
- Liability and indemnification in all Modules.

To avoid any potential misinterpretation and conflicts, CIPL would recommend to the extent possible, to replicate the language of the relevant GDPR article instead of modifying the language within the SCC.

In addition, under Modules 2 and 3, the SCC should not impose additional obligations which go beyond those applicable under the GDPR, (except as they relate specifically to risks posed by the transfer, such as law enforcement access) on processors or sub-processors. This means that the provisions on Data Protection Safeguards in Clause 1 should mirror the obligations imposed on processors under the GDPR and in particular Article 28 and should not expand those obligations.

As with the current SCCs, the New SCCs should apply a tiered process for liability and third party beneficiary rights for Modules 2 and 3, where a direct claim against the importer (or processor) can only be brought if the data subject cannot obtain recourse from the exporter because it has ceased to exist.

Finally, the New SCC should clarify that the term "local law" is to be interpreted in a substantive manner throughout the SCC, consistent with Recital 41 GDPR which expressly refers to the case law of the CJEU and ECHR. Notably, where the ECHR refers to surveillance measures prescribed by law, it applies a substantive interpretation that is not limited to the civil law tradition of acts of parliament and statutory provisions, but that expressly covers unwritten standards.[8]

Summary of CIPL recommendations:

- **Replicate the wording of the GDPR in the SCC to ensure consistency;**
- **Do not impose additional obligations on processors and sub-processors in Modules 2 and 3;**
- **Apply a tiered process for the exercise of third-party beneficiary rights against processors similar to that of the current SCC; and**
- **Clarify "local law" is to be interpreted in accordance with Recital 41 GDPR.**

1.5 Improve format of the New SCC

As the New SCC are often used together with other contracts and to align with the wording of Article 46 (c) GDPR, CIPL recommends renaming them as "Standard data protection clauses."[9]

[8] See *Kruslin v. France*; *Chappell v. the UK*.

[9] CIPL White Paper on Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR, August 2019, (highlighting that this may create confusion for organisations). 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

For purposes of clarity, CIPL would recommend providing, in addition to the current modular template, templates covering each scenario to provide as much flexibility as possible to organisations.

In addition, Clause 6(b) of the docking clause should be rephrased to provide that, upon accession, not only does the accessing entity have the rights and obligations of the exporter or importer, but also that the other parties will have the relevant rights and obligations in respect of the new entity as well.

Finally, given the complexity of the different case scenarios, the EU Commission should provide a FAQ with different use cases to better assist organisations identify their situation under the New SCC, such as for instance:

- Further clarify the notion of "transfer" and how it applies in complex digital supply chains. Given the realities of the data processing service industry, there will most often not be one unique act of "transfer" of data between party A and party B, but rather ongoing and instantaneous data flows between multiple stakeholders;

- Explain the interplay between Chapter V and Article 3(2) GDPR with practical use cases;

- In Module 1 (C to C), provide clarity on how the GDPR applies to the importing controller;

- When an exporter and an importer have multiple roles as part of the same contractual relationship, they should be allowed to sign a single set of SCC covering the different scenarios, with multiple versions of Annex I.B. This would be the case, for example, where a hosting provider located in India acts as an importing processor to host EU data (Module 2), and as an importing controller to provide certain value-added services (Module 1);

- The docking clause in Clause 6(a) should be formalized by having one party complete and sign the SCC Annexes;

- Section I, Clause 1(b) defining the parties to the SCC should enable one party to be appointed to sign on behalf of other exporters/importers (e.g., its affiliates);

- Explain and provide examples of "intermediary" in Clause 1(b)(ii); and

- Organisations should be able to include links and references in the SCC to online tools and resources (such as a web page) to enable a real-time update of the SCC in case of modification to the processing. This would be particularly relevant to update the Annexes (in particular Annex III "List of Sub-Processors") or to add new parties under the docking clause.

Protection Clauses" or "SDPC" in the context of third-country transfers, while SCC are mentioned in the context of processor obligations.

Summary of CIPL recommendations:

- **Rename SCC as Standard Data Protection Clauses in accordance with the GDPR;**
- **Provide templates covering each module, in addition to the current modular template;**
- **Adjust the wording of the docking clause; and**
- **Provide a FAQ answering most common questions on the SCC.**

1.6 Provide for more flexibility in interactions with other contracts

SCC are contractual provisions that are generally not executed in isolation, but in the context of wider commercial and contractual relationships between the parties. They are therefore incorporated into commercial contracts that always contain indemnity and liability clauses and also possibly contain confidentiality, security or audit clauses, for example.

Section I – Clause 4 "Hierarchy" provides that in case of conflict with an existing agreement, 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 requirements. For example, Clause 1(5)(d) of Section II provides that a data importer must notify a data breach "without undue delay" while a data exporter with the former SCC in place supplemented by the necessary provisions required by Article 28 GDPR may have imposed a stricter timeline (e.g., reporting within 24 hours). Strictly applying the New SCC would require the reopening of the timeline without any benefit for GDPR compliance.

Clause 1(c) provides that SCC shall not be modified, including directly or indirectly, by the provisions of a broader contract in which they may be included. CIPL underlines that there is a tendency to follow the SCC literally and some absolutist positions even consider that merely changing the language or format of the SCC would "contradict" the Clauses leading to endless and counterproductive discussions. A mere resequencing of clauses, 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 document. In order to address this, CIPL recommends amending Clause 1(c) to provide that the provisions of other contracts shall not "ignore, exclude or contradict, directly or indirectly, the protections provided by the Clauses" or similar language allowing for more flexibility of the New SCC in interactions with other contracts while preserving their essential effect.[10]

In addition, Clauses 7 and 8 on liability and indemnification may not be necessary in the New SCC as Article 82 GDPR already addresses compensation of the data subject and the relationship between the parties. CIPL recommends that these Clauses be removed and be replaced with the wording of Article 82 GDPR.

[10] Recital 3 of the Commission Decision should also be amended accordingly.

Summary of CIPL recommendations:

- **Clarify that SCC prevail over existing agreements without prejudice to existing provisions going further than the SCC;**
- **Amend Clause 1(c) to provide that the provisions of other contracts shall not "ignore, exclude or contradict, directly or indirectly, the protections provided by the SCC"; and**
- **Replace Clauses 7 and 8 on liability and indemnification by the wording of Article 82 GDPR.**

1.7 Reconsider timing for implementation of New SCC

Considering that the current SCC have been used for a decade in thousands of contracts, providing a high level of protection and safeguards substantially similar to the New SCC, and considering that organisations are required to verify if supplementary measures should be in place following the Court decision, the one-year request to update all SCC appears extremely burdensome.

CIPL would advise against imposing a mandatory time period for the implementation of the New SCC or would recommend a period no shorter than three years for longer term contracts that are not up for renewal. A grandfathering clause for those existing SCC should also be added. CIPL believes that a one-year deadline will not just challenge large companies with potentially thousands of data flows, but also SMEs with fewer available resources. In addition, it is key to consider that the implementation of the New SCC is much more than a contracting update exercise. It also involves substantive discussions with third parties and possible reopening of commercial discussions that may take substantial time to close as well as flowing-down the same terms to (sub-) processors in case of onward transfers.

CIPL highlights that there is ample room for such a flexible approach, especially since the current SCC have not been invalidated by the CJEU and still provide appropriate safeguards for transfers of personal data outside the EU.[11] Not limiting the implementation deadline would enable organisations to replace the current SCC as part of their normal course of business[12] as opposed to setting up a rushed project plan that may be counterproductive and unnecessarily disruptive to the ordinary course of renewal cycles creating duplicative work without commensurate enhanced protection as a justification. This would enable SCC to remain in place for the duration of the agreement they are attached to (except in case of substantial change in the processing operations).

[11] See paragraph 149 of the Court Decision.

[12] This would also be in line with the previous C to P SCC. See Article 7 of Commission Decision 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 of the European Parliament and of the Council https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&rid=4

Summary of CIPL recommendations:

- **Do not impose a mandatory time period for the implementation of the New SCC or, if any, provide for a timeframe no shorter than three years; and**
- **Add a grandfathering clause for the current SCC.**

2. Specific Comments on Section II of the SCC - Obligations of the parties

Clause 1- Data Protection Safeguards

2.1 Align requirements of the New SCC on security of processing and breach reporting to GDPR

In Modules 1, 2 and 3, Clause 1(5)(c) and Clauses 1(6)(c) respectively require the importer to take appropriate measures to address a data breach, including measures to mitigate its possible adverse effects. However, this obligation is not explicitly stated in the GDPR. It can, at best, be indirectly inferred from Article 33(5) GDPR, which imposes an obligation on the controller to document data breaches comprising its effects and the remedial action taken, which is a different wording to that of the New SCC.

In Module 1, Clause 1.5(d) and (e) place an express notification obligation on the importer to notify the DPA, the exporter and, as the case may be, the data subjects of a breach that is likely to result in significant adverse effects. This reporting standard is different from that under the GDPR which requires notification to the DPA "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (Article 33(1) GDPR) and notification to the data subjects when the breach "is likely to result in a high risk to the rights and freedoms of natural persons" (Article 34(1) GDPR). The New SCC should fully align with these GDPR standards and with the guidance already provided by the EDPB in order to avoid any conflict of interpretation or confusion. Hence, CIPL recommends that the wording of Clause 1(5)(d) and (e) are amended in a manner that introduces the criteria mentioned in Article 33(1) and Article 34(1) of GDPR.

In Modules 2 and 3, Clauses 1(6)(c) provide that in the event of a data breach, the importer shall also notify the exporter and provide all the details mandated by Article 33(3) GDPR. CIPL highlights that this would exceed the requirements of 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 of 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 to either remove the requirement to provide all details of the breach as mandated by Article 33(3) of GDPR – as it does not apply to the processor – or qualifying Clauses 1(6)(c) by adding "to the extent reasonably feasible taking into account the nature of the processing and the information available to the data importer." This Clause also provides that the data importer shall notify the data exporter "without undue delay." This does take into account the fact the parties may have agreed to apply a specific breach notification delay in a separate agreement. In that case, this specific breach notification delay should prevail over the wording of the SCC.

Additionally, Module 1 Clause 1(5)(a) and Module 2 Clause 1(6)(a) are not aligned with Article 32 GDPR as they fail to reference important considerations such as the state of the art, the costs of implementation

or the risks of varying likelihood and severity for the rights and freedoms of natural persons. CIPL recommends the SCC quote the exact wording of Article 32 GDPR to avoid introducing a different set of criteria for the assessment of security risks that would lead to altering the existing security assessments, vendor due diligence modules and questionnaires. This would impose a different standard for counterparties outside of the EEA, beyond the GDPR requirements.

Finally, in Modules 1, 2 and 3, the reference to the obligations of the parties "during the transmission" should be clarified. This term may trigger varied interpretations in a technical context.

Summary of CIPL recommendations:

- **Fully align with Articles 33 and 34 GDPR for breach reporting requirements;**
- **In Modules 2 and 3, remove the requirement for the processor to provide all details of the breach as mandated by Article 33(3) of GDPR or qualify Clauses 1(6)(c) by adding "*to the extent reasonably feasible taking into account the nature of the processing and the information available to the data importer*";**
- **In Module 1 Clause 1(5)(a) and Module 2 Clause 1.(6)(a), align wording with Article 32 GDPR to include considerations on state of the art, costs of implementation or the risks of varying likelihood and severity; and**
- **Clarify the term "transmission."**

2.2 Make pseudonymisation requirements more practical

In Modules 1, 2 and 3, Clauses 1(5)(a) and 1(6)(a) respectively require that in case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the exporter. CIPL believes the requirement of exclusive control to be impractical. This assumes that pseudonymisation will always be performed by the exporter. At the same time, it excludes the offer by the importer of pseudonymisation as a privacy enhancing feature, e.g., of a service which could benefit the exporter, especially if such exporter may not have the capability of doing it itself, as it is often the case for SMEs. For instance, some cloud providers propose tokenization features where the additional identifying information is kept separate so that only the exporter is able to get to the real data behind the token. In addition, in Module 3, the exporting processor would not be in possession of the additional information, or the additional information would not be in control of either the data exporter or data importer. For example, controller customers (who are not the exporters) may hold additional information about the data subject to re-identify him/her, such as an ID number. In other cases, neither the exporting processor nor the importing sub-processor will control the pseudonymisation where an industry standard technique (such as hashing) is used. CIPL therefore recommends that the word "exclusive" be removed from this paragraph and that the obligations only apply to the extent applicable.

Summary of CIPL recommendations:

- **Rephrase Clauses 1(5)(a) and 1(6)(a) in Modules 1, 2 and 3 to remove the obligation of the exclusivity of control in the additional information; and**
- **Clarify that the obligations related to pseudonmysation only apply to the extent applicable.**

2.3 Further streamline the onward transfers provisions

The New SCC introduce a framework for onward transfers which is more restrictive than that allowed by the GDPR and may unduly impact existing data flows. All Modules should be expanded to allow onward transfers on the basis of Chapter V GDPR. This change would also ensure that economic reality is respected where importers have their own business arrangements with their processors. To force these processors to join every single New SCC independently would constitute an undue administrative burden on all parties. In addition, for better consistency purposes, the Commission should refrain from adding new language to explicit consent for onward transfers. Instead, CIPL suggests that the New SCC refer to the requirements for transfers under explicit consent already available under Article 49 (1) GDPR for derogations.

Summary of CIPL recommendations:

- **Modify onward transfer provisions to expand them to take place on the basis of all the transfer provisions of Chapter V GDPR; and**
- **Remove language on explicit consent for onward transfers.**

2.4 Review the audit provisions

CIPL recommends that, as a matter of practicality, Clauses 1(9)(d) in Modules 2 and 3 limit the audits to "not more than once a year" and/or "unless necessitated by exceptional circumstances." This would align to the terms of existing commercial agreements that generally contain such language. In addition, CIPL recommends to include that audits should be subject to and preceded by an agreement between the parties defining the scope, security, confidentiality, time and duration of the audit which reflects current commercial practice (for example, it would not be appropriate if a direct competitor of the importer were to be appointed by the exporter as its auditor). CIPL also highlights that sub-processors are generally not able to permit audits of their facilities and systems from all controllers on whose behalf they ultimately process personal data as for some sub-processors, this could amount to organising audits for thousands or even tens of thousands of controllers. 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.

Summary of CIPL recommendations:

- **Redraft the audit clause to align with current commercial practices; or**
- **Make this clause optional in the SCC.**

Clause 2 - Local laws affecting compliance with the Clauses

The Court Decision has the unfortunate effect of requiring industry to make novel assessments and to provide legal advice on the laws of the countries where they conduct business, to make onerous representations and to take blind commitments vis-à-vis their business partners on this basis. It cannot be overstated that this is a significant shift compared to the current SCC that must be fully taken into account in their updated version. On this basis, the EU Commission should make clear that the New SCC do not require organisations to assess a country's rule of law and practices to verify whether it respects "the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR." Instead, any assessment should be explicitly limited to assessing whether the New SCC provide an adequate level of protection in relation to a specific data transfer in the specific circumstances at hand. Organisations understand that their role is limited to assessing the risk of a specific transfer by itself taking into consideration all the specific circumstances of the transfer which may include consideration of applicable local laws.

CIPL welcomes the approach taken in Clause 2(b) in qualifying the warranty they provide on the law applicable in the country of destination but would welcome a more specific reference to the GDPR risk-based approach in the context of the exporter's obligations under Clause 2 (see Section 1).[13] CIPL would also suggest that the EU Commission consider including the following criteria in performing the risk assessment: (i) the categories of data that are or are not, in practice, subject to requests from public authorities of the third country; and (ii) the rule of law and human rights approach of the third country.

Subject to CIPL recommendations in Section 1, it is important that Clause 2(a) define that the warranty provided by the parties should be amended so that it is clear that it takes into account the risk assessment referenced in Clause 2(b). As currently drafted, the two paragraphs potentially contradict each other, and the parties will be reluctant to give the warranty in paragraph (a) if their risk assessment reveals that the laws of the third country prevent the data importer from complying with the Clauses and that supplementary measures are needed.

In addition, the inclusion of the legal advisory and regulatory watch obligation on importers in Clause 2(c) should be based on reasonable efforts only and not on best efforts, which is a very high standard to achieve. Further, the requirement in Clause 2(d) to document the risk assessment and make it available to the competent DPA upon request is only acceptable to the extent that these are assessments based on reasonable efforts, and without liability attached to the findings as neither party is in a position to make any authoritative determination or representation as to the substance and interpretation of applicable

[13] The EU Commission and the EDPB may also wish to consider proposing a non-mandatory template to assist organisations, in particular SMEs, in performing these risk assessments.

laws. This would also align with the wording of Clause 1 ("The data exporter warrants that it has used reasonable efforts to determine that the data importer is able to satisfy its obligations under the Clauses"). Similarly, the obligations of the parties would be more accurately reflected if they enabled or permitted compliance with the Clauses, rather than if they ensured compliance with the Clauses which is, by definition, unachievable.

It is also key that the wording of the SCC and that of the EDPB Recommendations are aligned to avoid confusion.[14] The SCC currently provides that the data importer carries out the assessment, while as per the EDPB Recommendations, the exporter is responsible for completing the assessment with the collaboration of the importer where appropriate, which is more aligned with the GDPR. In the same vein, Clause 2(f) requires the exporter to identify appropriate measures to be adopted by the parties to address the situation where the data importer cannot fulfil its obligations under the Clauses. CIPL recommends clarifying that the exporter has to mandate "appropriate measures" which can "reasonably" be implemented by the importer as this provision cannot be a 'carte blanche' for the exporter to require any changes to the processing, no matter how impractical or expensive. In this context, CIPL recommends taking inspiration from Articles 25 and 32 GDPR subjecting the definition of data protection by design and by default measures as well as security measures respectively to, among other criteria, the state of the art and the cost of implementation.

Clause 2(f) further requires the exporter to notify its competent DPA where the importer may not be able to comply with the SCC. This requirement introduces some confusion, as it applies indistinctly where the exporter decides to continue the transfer after having implemented appropriate supplemental measures to remedy the issue or mitigate the risks as well as where it decides to suspend the transfer. This goes beyond the Court Decision which only requires notification to the DPA where supplemental measures are insufficient, but the exporter wishes to continue the transfer.[15] In addition, in practice, this provision is more likely to discourage importers from informing exporters about the issues they experience and potential changes in local laws and practices rather than improve transparency to the exporter. In addition, DPAs run the risk of being overwhelmed with notifications that would not add any value to the protection of individuals. CIPL underlines also that the GDPR removed the obligation for organisations to notify the DPA before transferring data outside of the EU that this provision would somehow tend to reinstate.[16] At the same time, data transfers would be safeguarded by the appropriate supplementary measures applied to the transfer as per the arrangements between the exporter and importer. CIPL therefore recommends limiting the notification to the DPA only where the exporter decides to suspend the transfer or terminate the contract, which would alert the DPA of possible inappropriate behaviours and provide a basis for looking more closely at the importer's arrangements with other exporters.[17]

[14] CIPL underlines the importer is often part of a complex ecosystem where the obligations of each stakeholder regarding the risk assessments are yet to be clarified (i.e. relation of a supplier with its own vendors or of a platform with its different merchants).
[15] CIPL understands the EU Commission's intent to involve the DPA as soon as possible and before the organisation becomes aware that supplemental measures may be inefficient. In case of a personal data breach however, notification to the DPA is only required when the organisation becomes aware of the breach.
[16] See recital 89 GDPR recognising that notifications do not generally contribute to improving the protection of personal data.
[17] Recital 21 of the draft Commission Decision should also be modified accordingly.

Finally, Clause 2(f) provides the exporter with the possibility of terminating the contract in case it suspends the problematic transfer. This should be further nuanced as total termination of the contract may be disproportionate. If the importer is unable to comply with the Clauses only with respect to a limited number of data subjects, or in the context of a single processing activity, then the suspension of such transfer(s) should suffice where that is practicable. Otherwise, any single government data access request to a single record could endanger entire contractual relationships in a disproportionate manner. The same comment applies to Section III, Clause 1(b) on non-compliance with the clauses and termination.

Summary of CIPL recommendations:

- **Clarify that organisations are not required to assess a country's rule of law and practices to verify whether it respects "the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society";**
- **Modify Clause 2(b) to include that the criteria of the risk assessment could also include (1) the categories of data that are or are not in practice, subject to requests from public authorities of the third country; and (2) the rule of law and human rights approach of the third country;**
- **Modify Clause 2(a) to provide that the warranty provided by the parties takes into account the risk assessment referenced in Clause 2(b);**
- **Modify the wording of Clauses 2(c), 2(d) and 2(f) to include a standard of reasonableness;**
- **Limit the notification to the DPA of Clause 2(f) to only where the exporter decides to suspend the transfer or terminate the contract; and**
- **Remove the possibility for the exporter to automatically terminate the contract in case in Clause 2(f).**

Clause 3 - Obligations of the data importer in case of government access request

Clause 3.1 provides that the importer agrees to promptly notify the data subject, where possible, when it receives a legally binding request or becomes aware of any direct access by a public authority. CIPL underlines that providing this information would only be possible in the case where the importer has a direct relation with the data subject, i.e., when the importer is the controller in Module 1. It may also be unrealistic for importers to inform data subjects (for Module 1 only) and exporters of all the requests they receive or access that they become aware of without any regard as to whether those requests would actually result in violating EU law. This clause should be limited to informing the data subject only in case these access requests are problematic vis-à-vis compliance with the SCC.

CIPL recommends that the EU Commission also provide for delayed notifications to the data subject or the exporter, especially in cases where it is justified by countervailing interests such as public security of public safety arising from counterterrorism and child safety for instance. Delayed notifications still enable individuals to exercise their rights. CIPL underlines also that in some emergency circumstances, any notification or obtaining of a waiver will be impossible.

The obligation for the importer in Clause 3(1)(d) to keep the information pursuant to a government access request for the duration of the contract may be disproportionate. This is especially true in long contracts as it may require the retention of personal data for longer than necessary for actual business purposes. CIPL recommends limiting the term of retention to "as long as reasonably necessary to protect the legal claims of the Parties and the interests of the data subjects concerned." In addition, CIPL believes that the information which the importer is required to preserve should be made available to the exporter upon request, and then to the DPA further to a request placed directly on the exporter. This approach is consistent with the accountability principle and the contractual arrangements that exist between the exporter and the importers. In addition, Clause 1(9) already places a general obligation on importers to document compliance and make such documentation available to the DPA upon request.

Clause 3(2) requires data importers to review the legality of the request for disclosure, to exhaust all available remedies to challenge it and to request interim measures under the laws of the country of destination.[18] CIPL understands that this provision also includes an assessment of a lack of reasonable merit of the request, as well as the determination of what would be the most appropriate course of action (e.g., injunctive relief). Otherwise, importers would be expected to systematically exhaust all possible avenues to challenge a request even if the request appears perfectly legitimate and justified. In addition, the commitment to challenge a request should be predicated on whether there is a conflict with EU law, not solely on whether there are grounds to do so in the law of the destination country. This should also enable importers to prioritise legal challenges for the most problematic requests that are patently unlawful, illegitimate or excessive. In addition, in line with the GDPR's risk-based approach, CIPL recommends that importers are enabled to perform an assessment as to the level of risk of the request on the concerned individuals' rights and freedoms, including likelihood and severity of harm, before engaging in time and resource intensive legal proceedings. Finally, CIPL recommends that it should be made clear that such challenges be based on their cost and feasibility.

The best effort obligation or the obligation to communicate the greatest possible amount of information under Clause 2(c), Clause 3(1)(b) and (c) are very high standards to reach for the importer. This may discourage non-EU importers from partnering with EU organisations. Imposing a reasonable effort may have less adverse legal effect, while leading to the same results in practice as the importer has generally a strong business interest in ensuring that the business relationship with the exporter continues. The importer could only be required to provide a summary of the requests specifically related to the exporter's data (especially in cases where it is not possible to share the precise details of a specific request due to legal restrictions). In addition, in order to present information in a consumable form, including in published transparency reports, the obligation should be to make relevant information available, not the greatest amount of information possible. Alternatively, it should be limited to information requests that are broad, excessive or disproportionate.[19]

[18] CIPL highlights that this language is particularly problematic in a C to C context where the importer is processing the data for its own benefit and must exercise its own discretion.
[19] Recital 22 of the draft Commission Decision should also be modified accordingly.

Summary of CIPL recommendations:

- **Narrow the scope of Clause 3.1 to notify the data subject only when the data importer has a direct relationship with the data subject and when the access requests do not comply with the SSC;**
- **Include a possibility of delayed notification in Clause 3.1 to address exceptional circumstances;**
- **Limit the obligation for the importer in Clause 3(1)(d) to keep the information, pursuant to a government access request for the duration of the contract, to "as long as reasonably necessary to protect the legal claims of the Parties and the interests of the data subjects concerned";**
- **Modify Clause 3(2) to enable data importers in reviewing the legality of government data request to assess the reasonable merit of the case, to determine the most appropriate course of action and to take into account conflict with EU law, level of risk on individuals, cost and feasibility; and**
- **Apply a reasonable standard to the obligation to disclose information under Clause 2(c) and Clauses 3(1)(b) and (c).**

Clause 4 – Use of sub-processors

Despite the two different options in the headings, Clause 4(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 III which therefore become 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.

Clause 4(c) requires that the importing processor provide a copy of the sub-processor agreement to the exporter upon request. Because these can be included in wider commercial agreements, CIPL recommends including the option for the importer to redact that information from the sub-processor agreement to protect confidential information. CIPL recommends mirroring the language contained in Clause 1(2)(c).

While CIPL welcomes the inclusion of a docking Clause in the New SCC, CIPL highlights more generally that in case of onward transfer to a sub-processor which agrees to be bound by the SCC, accession to SCC in practice by additional parties may be quite difficult to achieve because the SCC will often be incorporated into broader contracts which will not be directly binding on sub-processors.

In Clause 4(b) in Modules 2 and 3, CIPL further notes that the data importer is required to "ensure that the sub-processor complies" with the data importer's obligations. This is an unachievable standard as previously noted in our comments regarding Clause 2. Accordingly, CIPL recommends that the EU Commission consider that it is sufficient that the data importer remains fully responsible for the performance of the actions of the sub-processor's obligations under section (d).

Summary of CIPL recommendations:

- **Establish a clear distinction between the specific and general authorisation to sub-processing in Clause 4(a);**
- **Enable the processor to redact information from an agreement to protect confidential information; and**
- **Remove provision in Clause 4(b) that the data importer is required to "ensure that the sub-processor complies" with the data importer's obligations.**

Clause 6 – Redress

Clause 6(a) provides that the importer shall inform data subjects in a transparent and easily accessible format of a contact point authorised to handle complaints or requests and shall promptly deal with any complaints or requests by a data subject. CIPL highlights, however, that this provision is only relevant and applicable if the importer is the controller, i.e., Module 1 (C to C) as only controllers have the duty (and are in the actual position) to provide information on requests and complaint handling to the data subjects. In C to P and P to P scenarios, the importing processor acts on the instructions respectively of the exporting controller or the exporting processor regarding handling of requests and complaints of data subjects. Therefore, CIPL recommends that Clause 6(a) be amended by introducing a provision limiting the application of this Clause to Module 1 (C to C).

Clause 6(d) requires data importers to accept abiding by decisions applicable under EU or member state law. CIPL welcomes this commitment as a mechanism for ensuring that data subjects have an effective right to redress. However, CIPL would suggest clarifying that this obligation would apply notwithstanding the right of the importer to challenge such decisions in court and to exhaust all available legal remedies.

Summary of CIPL recommendations:

- **Amend Clause 6(a) to provide that the importer shall inform data subjects of a contact point for complaints or requests to limit it to Module 1; and**
- **Clarify in Clause 6(d) that data importers are bound by applicable decisions notwithstanding their right to challenge such decisions in court and to exhaust all available legal remedies.**

Clause 9 – Supervision

Clause 9(a) provides that the DPA competent for exporters not established in the EU under Article 3.2 GDPR is that of the Member State where the data subjects whose personal data are transferred under the clauses (in relation to where the offering of goods or monitoring are located). CIPL underlines that, in practice, there will be several countries involved. In this situation, the competent DPA should be that of

the country where the majority of individuals are located or, alternatively, the Member State in which the entity's Article 27 GDPR Representative is located.

In Clause 9(b), the importer's acceptance of the jurisdiction of the competent DPA should be subject to the GDPR's rules on DPA competence, including the One-Stop-Shop mechanism to avoid any potential conflicts as to which DPA has jurisdiction over a particular transfer. This is also important to avoid parties being subject to overlapping enforcement contrary to the principle of non bis in idem.

Summary of CIPL recommendations:

- **Clarify that the competent DPA under article 3.2 GDPR should be that of the country where the majority of individuals are located or, alternatively, the Member State in which the entity's Article 27 GDPR Representative is located; and**
- **Clarify that competence of the DPA is subject to the One-Stop-Shop mechanism.**

3. Specific Comments on Section III of the SCC – Non-compliance with the Clauses and termination

The decision to suspend a data transfer could have far reaching consequences extending beyond the strict remit of data protection and shall therefore be duly weighed beforehand. In addition, full harmonisation and consistency in approaches is particularly key. As a consequence, in some instances, it may be necessary for the exporter to consult with the DPA, the EU Commission or with other regulators (securities, anti-money laundering, health, national intelligence, etc.) in charge of supervising activities that may be impacted by the suspension of the transfer.

4. Comments Specific to Module 1 – C to C

Clause 1(1) on "Purpose" requires that the importer obtain the data subject's consent to process the data for purposes that are incompatible with the transfer description in Annex I.B. CIPL recommends, however, for better alignment with the GDPR that the New SCC allow the data importer to use the appropriate GDPR legal basis (Article 6 or Article 9 GDPR, as applicable), which are not limited to consent.

Clause 1(2)(a) on "Transparency" requires the importer to provide information to the data subjects either directly or through the exporter. CIPL believes, however, that because the importer is a controller, either the importer is subject to the GDPR directly under Article 3.2 or, if the importer is not subject to the GDPR, then these transparency requirements are already set forth contractually. Where the importer and exporter have contractually agreed for one of them to take on the transparency obligation (as permitted by 1.2(a)), the provision should relieve a controller of liability if the other Controller has agreed to take on that obligation.

Clause 1(2)(a)(iii) requires the importer (controller) to disclose information to individuals on the identity of third-party recipients of the data and the purpose of disclosure whereas Article 13(1)(e) GDPR only requires identification of categories of recipients. Hence, CIPL recommends the alignment of Clause 1(2)(a)(iii) to the wording of Article 13(1)(e) of GDPR.

Summary of CIPL recommendations:

- **Modify Clause 1(1) to include all GDPR legal bases and not only consent; and**
- **Review Clause 2(a) to align with GDPR wording.**

5. Comments Specific to Module 3 – P to P

Clause 1(1)(a) on instructions provide that the exporter has informed the importer that the exporter acts as a processor under the instructions of the controller or controller(s) listed in Annex I.A. CIPL highlights that depending on the business relationship with the controller(s), this may be neither feasible in practice nor even desirable or necessary in theory as for the importing sub-processor, the identity of the controller may not matter at all (this may amount to disclosing lists of customers to the importer which may raise confidentiality issues). Further, whether the exporter is a controller of its own or a processor acting on someone else's behalf may be irrelevant as in both cases the importing sub-processor will equally act on the exporter's instructions and under its responsibility. Therefore, CIPL suggests redrafting the Clause to better reflect the business realities and to delete the identity of the controller for P to P transfers from Annex I.A "Identity of the Parties."

In addition to the fact that the sub-processor may not know the controller, in several instances, the New SCC appear to create an artificial relationship between the controller and the sub-processor by imposing direct obligations between them. Doing so goes beyond the requirements of the GDPR, is not aligned with contractual law and relies on the wrong assumption that the controller and the sub-processor may be in direct contact, which may not be the case in most digital supply chains. The New SCC does not take into account the fact that these obligations and the corresponding risks are already managed directly by the first rank processor acting on behalf of the controller. For instance, the customer (EU controller) of a SaaS service (EU processor) hosted on an IaaS cloud platform (non-EU sub-processor) does not give direct instructions to the cloud platform and there is no direct contractual relationship between them. Instead of creating direct obligations between the controller and the sub-processors, the obligations should flow down from the controller to the first rank processor down to the subsequent sub-processor(s), in a way that mirrors the relationship between the processor and the controller as set forth in Article 28 of GDPR. CIPL recommends removing these problematic provisions from the New SCC as Module 3 is likely to become the standard for data processing and transfer terms across long sub-processing chains especially in B2B scenarios.

For instance, such would be the case for the following Clauses:

- Obligation for an importing processor to process the personal data only on documented instructions from the controller and any additional documented instructions from the exporter (Clause 1(1)(b));
- Obligation for the importing sub-processor to notify the controller of a data breach (Clause 1(6)(c));
- Obligation for an importing sub-processor to only disclose personal data to a third party on the basis of documented instructions from the controller (Clause 1(8)).
- Obligation for an importing processor to deal with inquiries from the controller (Clause 1(9)(a));

- Obligation for an importing sub-processor to permit audits by the ultimate controller (Clause 1(9)(c) and(d));
- Obligation for the sub-processor to obtain a prior specific authorization from the controller to engage further sub-processors (Clause 4(a));
- Obligation for the importing sub-processor to notify, if appropriate, the controller when receiving a request from a data subject (Clause 5 (a) and (b)).

CIPL therefore recommends to revisit these provisions in line with the requirements of Article 28 (4) GDPR rather than to create a different framework for non-EU based sub-processors.

In a similar vein, the sub-processor should not be required to engage with the data subject as only the controller is in a direct relationship with the data subject. Clause 1(3)(b) provides that the parties shall provide a copy of the clauses to the data subject upon request. This Clause is not adapted in P to P contexts as neither parties are in a direct relationship with the data subject. The parties have no obligations with respect to data subject rights other than indirectly assisting the relevant controller as appropriate through other processors up to the first rank processor.

Finally, given these clauses are also intended to serve the purposes of Article 28 GDPR (i.e., data processing and sub-processing agreements), the EU Commission should ensure that all provisions (and in particular the qualification of the parties) are adapted to a P to P relationship including when the parties are both importers within the meaning of the New SCC. However, the current drafting does not always appear to be adapted in that scenario as well.[20] Similarly, the construct of this module wrongfully assumes that the exporter is always located in the EU whereas this may not be the case when the GDPR applies by virtue of Article 3.2 GDPR.

Summary of CIPL recommendations:

- **Modify Clause 1(1)(a) to remove the obligation to provide the identity of the controller, including Annex I.A of the "Identity of the Parties";**
- **Remove provisions in Module 3 creating a direct relationship between the sub-processor and the controller as well as obligations to engage directly with the data subject; and**
- **Review Module 3 to ensure that the SCC provisions are adapted to P to P scenarios when both parties are importers.**

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

[20] For example, Clauses 1(1)(a)(b) and (c) in the instructions do not appear to work as well under Article 28 GDPR.