ITI Promoting Innovation Worldwide

10 December 2020

ITI Comments to the European Commission Implementing Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries

ITI is the global voice of the tech industry. Our 74 member companies include leading innovation companies operating worldwide value chains and active through all segments of the technology sector. Privacy and user trust are central to our member companies' businesses and global operations. Our industry shares the goal of safeguarding privacy with the European Commission, and together with our members, we are working with European and global institutions as well as supervisory authorities (SA) around the world on key data protection and privacy issues, including the General Data Protection Regulation (GDPR).

ITI endorses strong protections for personal data transfers to third countries, and we are pleased to provide our input to the European Commission's *implementing decision on standard contractual clauses (SCCs) for the transfer of personal data to third countries*. We appreciate the European Commission's efforts in modernizing and refining the SCCs to reflect the *Schrems II* judgment and welcome positive changes to incorporate additional safeguards. We also welcome the introduction of the new SCCs for processors in the annex to cover diverse situations.

We encourage the Commission to consider how all stakeholders including public authorities, law enforcement, consumer groups, academics and research bodies, in addition to SA and industry, should come together to reflect and explain the role data flows play in underpinning our modern lives. ITI recommends that the Commission facilitate the smooth negotiation of an EU-US enhanced Privacy Shield agreement, fully align the SCCs with the GDPR's risk-based approach (we advocate that the draft European Data Protection Board (EDPB) recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data should also be so aligned), and provide a sufficient transition period. Our detailed comments provide recommendations to specified clauses that we believe would benefit from further refinement. We look forward to an exchange on these ideas and remain at your disposal for continued discussions.

ITI General Recommendations

Adopt an approach that takes into account privacy, security and economic considerations. The following recommendations reinforce the view that solving the crux of the issues raised by the Court of Justice in *Schrems II* — i.e., the rules under which government authorities in the US or other third countries can access to European data for law enforcement or national security purposes — requires an approach that cannot entirely revolve around imposing additional prescriptive measures on companies who are grappling with difficult conflicts of laws. In the transatlantic context, it is more important than ever that the EU and the US continue and swiftly conclude their negotiations for an enhanced data transfer agreement respecting European citizens' fundamental rights as well as the legitimate security and public safety interests of EU Member

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

States and foreign governments, while ensuring continuity of commercial activities. We encourage an approach that brings together EU data protection authorities and national security stakeholders to ensure intelligence sharing needs are included in the discussion, and also considers the equities of relevant of trade and economic actors across the EU. In particular, with respect to the negotiations for an enhanced transatlantic data transfers agreement between the US and EU, national security stakeholders who participate in intelligence sharing with US authorities are well positioned to help take into account the fact that US surveillance laws and practices have evolved significantly since 2016. ITI stands ready to support European and US policymakers (in both the current and incoming US administrations) to facilitate a smooth negotiation on a successor agreement to the EU-US Privacy Shield.

Explicitly Reinforce that the SCCs are Aligned with the GDPR's risk-based approach. ITI and our members have long supported the GDPR's risk-based approach to protecting personal data and we continue to advocate for an agile approach in our international data protection advocacy. We vigorously support SCCs and the other transfer mechanisms outlined in GDPR Article 46 as crucial tools for international data transfers that underline the role of data exporters in a risk-based assessment and choice of appropriate safeguards for transfers. We commend the Commission for embracing such a risk-based approach in paragraph 20 and Clause 2 (b)(i) Section II, which states that in considering whether the laws applicable to the data importer prevent it from complying with the clauses, the parties to SCCs should consider "any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred." This provision of the draft SCCs reflects well the need to consider the factual circumstances and context of a data transfer in order to fully assess any related risks.

In contrast, the draft EDPB recommendations caution against "subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with the EU standards." The EDPB recommendations do not reflect the importance of the specific, objective and measurable circumstances of a transfer in assessing risks, instead suggesting that organisations must adopt further safeguards even when there is only a theoretical possibility of potential access, which is at odds with the GDPR's risk-based approach and misaligned with the draft SCCs. We therefore recommend that the European Commission explicitly reference the GDPR's risk-based approach and accountability principle to prevent any interpretation incompatible with the GDPR, including the EDPB's draft guidance on supplemental measures, and further recommend that the European Commission continue enshrining the GDPR's risk-based approach and support aligning other relevant documents to the greatest extent possible.

Consider revising government request obligations to clarify obligations on data importers and exporters and better align with EDPB guidance. ITI recommends clarification of the responsibilities on data exporters to better determine whether the data export meets legal requirements and that neither party is obligated to provide legal advice to the other party. The draft SCCs and EDPB guidance are inconsistent on these points. For example, paragraph 21 of the SCCs seems to suggest that a data exporter must advise the competent supervisory authority when supplementary measures are put in place. Applied in every case, this seems impractical as well as unnecessary per the *Schrems II* decision, which stated such notice would only be required where supplementary measures are insufficient, and the data exporter wished to continue the transfer. We recommend revising the obligations for data importers, requiring them to preserve documentation and make

such available to the data exporter upon request, as well as to provide them to the SA under a request placed on the data exporter. This approach is consistent with the accountability principle and the contractual arrangements that exist between data exporters and importers. Particularly, Clauses 2 and 3 under Section II are not appropriate in a processor/controller relationship. For example, the controller should not be required to comply with instructions from the processor, and the processor should not be entitled, by 'suspending' the transfer, to effectively take exclusive possession of the controller's data. This could expose the controller to significant commercial and regulatory risks, if it no longer had access to its own data (e.g., relating to its own employees or customers).

Further, as proposed by the EDPB's recommendations, the data exporter is responsible for completing the assessment, with collaboration from the data importer, where appropriate (e.g., to advise on the laws in the third country). However, the draft SCCs in Section II, Clause 2(c) emphasise the role of data importers in carrying out the assessment. This apparent misalignment between the SCCs and the EDPB recommendations may lead to legal uncertainty for businesses relying on SCCs. We welcome the statement that the data importer has the role of cooperating with the data exporter but strongly urge that the EDPB recommendation and SCCs be aligned to clarify that the data exporter has the primary responsibility to carry out the assessment.

Provide clearer guidance explaining how controllers, processors and sub-processors should apply and use the SCCs in practice. We encourage the Commission to provide additional guidance regarding how entities should apply and use the modules in practice, including to clarify the proposed structure of the different modules, as it is unclear whether the 'multi-party' approach is intended to work horizontally (e.g., one controller to many processors) or vertically (e.g., controller, processor, sub-processor), or both. In particular, requiring controllers to be parties to the new SCCs when using Module 3 defeats the purpose of having processor to processor (P2P) terms, and is unworkable in the content of an infrastructure as a service (IaaS) model, or other digital supply chains, where customers (acting as processors) may have millions of end users (acting as controllers) and data subjects who are unknown to IaaS providers. In Module 3, the new SCCs appear to create an artificial relationship for the sub-processor with data subjects and controllers, by imposing direct obligations on the sub-processor to cooperate with, and notify controllers and data subjects in specific circumstances (for example, the new SCCs include an obligation for sub-processors to notify data subjects of governmental requests for personal data).

Given the existing rights for data subjects under GDPR to enforce rights against sub-processors, and the pre-existing contractual relationship between the data exporter and the controller, sub-processors should not have to interact with controllers or data subjects in P2P transfers. This type of interaction relies on the incorrect assumption that the controller and sub-processors are in direct contact, which will not be the case in many digital supply chains. As well as the practical obstacles of such dealings, this is likely to constitute a breach of the contractual commitments and confidentiality obligations that exist between the sub-processor and the data exporter. An explanatory preamble or FAQ document would be helpful here. We also recommend expanding the list of exceptions to allow onward transfers on the basis of agreements between the third-party and the data importer under all four modules.

Clarify provisions that have potential conflicts with the GDPR. The draft SCCs create duplicative responsibilities with the GDPR. In controller-to-processor (C2P) transfers (Module 2 of the new SCCs) and processor-to-processor (P2P) transfers (Module 3 of the new SCCs), the relevant data

exporter and data importer would have entered separate Article 28 data processing terms as required by GDPR. There is no need to replicate / duplicate the existing Article 28 obligations as the purpose of the SCCs is simply to address specific issues arising from transfers to third countries. Additionally, the draft SCCs conflict with the language of Article 28 of GDPR, creating an inconsistent set of obligations and raise the concern that the draft SCCs may supersede negotiated positions in data processing terms. For example, the draft SCCs include language around audit, notification of personal data breaches, use of sub-processors and storage limitation. These provisions conflict with Article 28 of GDPR, and the data processing terms between the parties, which parties may have negotiated considering service models (including IaaS). Similarly, there are commitments in the draft SCCs that require clarification in the context of other existing GDPR obligations, for example, a commitment on the data importer (as a processor) to identify inaccurate data. To avoid any misinterpretations and conflicts we recommend deleting these clauses from the draft SCCs in their entirety or amending them to reflect the language and commitments in GDPR.

Apply liability and third-party beneficiary rights carefully. The new SCCs should clarify and consider applying a 'tiered' process for liability and third-party beneficiary rights, where a direct claim against the importer (or processor) can only be brought if the data subject cannot obtain recourse from the exporter (or controller) (e.g., because it has ceased to exist). Only data importers which are data controllers (and not data processors) are under the duty to provide information of where to address complaints to the data subjects. Further, the SCCs should clarify that only tangible, real and actual damages to an individual, rather than hypothetical or theoretical damages, should be enforced and compensated by a court.

We note that liability of the SCCs in Section II, Clause 7 is stated as being "without prejudice to the liability of the data exporter under the GDPR." However, where there has been a breach of the GDPR and the SCCs, such breach should not entitle the data subject to claim compensation twice for the same damage. It should be clear, therefore, that any liability would be subject to any national laws preventing double-recovery. Further, SAs are not competent to deal with contractual issues (e.g., the validity and enforcement of a third-party beneficiary right). Compensation for damages should be considered if a GDPR sanction is imposed. If the clause is not carefully crafted, it could potentially deprive entities' contractual freedom without providing a benefit for data subjects. Data subjects will be tempted to pursue the party who they see as the 'easier' target (e.g., because it has deeper pockets) or conduct 'forum shopping', even if the complaint could satisfactorily be resolved by the exporter and/or EU controller (if different). This is particularly pertinent in Modules 2 and 3, since processors would generally have no direct relationship with the data subject. This is likely to increase risks for smaller companies that would be required to sign up for unlimited liability. We would welcome additional guidance in the SCCs on the possibility for parties to manage liability and indemnification commercially between them (without prejudice to data subjects).

Interpret local laws consistent with the GDPR and European court jurisprudence throughout the SCCs. In the context of the required assessments, we recommend that local law be interpreted in a substantive manner throughout the new SCCs. Doing so would be consistent with Recital 41 of GDPR, which expressly refers the application of case law of the CJEU and European Court of Human Rights (ECHR). Notably, where the ECHR refers to surveillance measures prescribed by law, it is worth recalling that 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 law (*Kruslin v. France; Chappell v. the UK*).

Allow sufficient time for transition. Under the European Commission's draft SCCs proposal, companies would need to phase out and replace all existing SCCs within 12 months following the adoption of the proposal. This would present small and large companies alike with the resource-intensive task of assessing each existing transfer and reworking contracts or potentially developing or activating alternative data and business continuity plans in many cases. So as not to impose disproportionate burden on companies, we recommend a longer transition timeline to ensure that stakeholders can properly conduct multi-country risk and data transfer analyses and adequately prepare their processes, procedures and compliance. Additionally, we recommend requiring exporters and importers to apply the updated SCCs only for new contracts signed after the date they become effective, allowing both new and old SCCs to remain valid during the transition period. The Commission should consider removing any suggestion that an organisation could lose the benefit of the grace period if other changes are made to the contract. This is especially important as the draft SCCs have a cross-sectoral impact. As technology companies work with clients across sectors, updating the SCCs' requirements and understanding new provisions will be a prerequisite first step. Therefore, a phased introduction plan setting a minimum reasonable timeline over a two-year period, similar to the GDPR implementation timeframe, should allow sufficient time for implementation and compliance.

ITI Detailed Recommendations

Draft Implementing Decision

- **Page 1 (para 3)** – We welcome the statement that the parties can include the SCCs in a wider contract and add other clauses. For completeness, the European Commission could reduce the uncertainty further by making it clearer that clauses that are concerned with process, rather than substance, do not contradict the clauses. An example would be a counterpart clause.
- **Page 3 (para 9)** – The clause should be more definitive – it currently says, "should also allow to fulfill the requirements." The European Commission should confirm the entities to which this clause applies (e.g., controllers, processors, sub-processors, etc.) and explain the caveats relevant to whether entities are or are not allowed to avail themselves of this option.
- **Page 6 (para 22)** – The primary requirement on a data importer with regards to government requests should be to provide that request to the data exporter (where possible) for the data exporter to challenge. In addition, the proposed requirement that data importers provide data exporters with aggregate information should be clarified; as written this requirement is vague, for example, the frequency of the phrase "in regular intervals." ITI recommends that company's transparency reports should be qualified for such definitions.
- **Page 6 (para 24)** – This clause suggests that organisations only get the benefit of the one-year grace period for implementing the new SCCs "if the contract remains unchanged." This could potentially cause difficulties if a contract needs to be updated but an organisation is not yet in a position to implement the new SCCs. The European Commission should consider

removing any suggestion that an organisation could lose the benefit of the grace period if other changes are made to the contract.

- **Page 7 (art. 1)** – We recommend adding that new SCCs are applicable to transfers of personal data from a controller or processor subject to the GDPR to a controller or processor not subject to the GDPR to avoid uncertainty.

ANNEX: Standard Contractual Clauses

Section I

Clause 1: Purpose and Scope

- **Page 1 Clause 1.b** – We recommend permitting one party to be appointed to sign on behalf of other data exporters/importers (e.g., affiliates). It is very burdensome to require multiple signatures when the parties may be using binding corporate rules (BCRs) or inter-company SCCs. Additionally, the signature block for the controller in Annex I should be removed, as it would not be a part to Module 3.
- **Page 1 Clause 1.b (ii)** – A data importer is defined as an entity in a third country receiving the personal data from the data exporter, directly or indirectly via an intermediary. We would encourage further clarification on the reference to intermediary and its interpretation.
- **Page 1 Clause 1.c** – As stated above, we welcome the statement that the parties can include the SCCs in a wider contract and add other clauses. The European Commission could make it clearer that clauses that are concerned with process, rather than substance, do not contradict the clauses. An example would be a counterpart clause. The Decision can further confirm that the new SCCs, like the current SCCs and Article 28 agreements between controllers and processors, can be used with additional clauses on business issues such as limitations of liability that will apply between the parties (provided that data subjects must always be fully compensated for any material or non-material damage suffered by them, as they would be under the GDPR). Particularly given the ambiguous new restriction on the parties agreeing to any other clauses that "indirectly" contradict the Clauses, confirmation of this point is needed to avoid causing any further confusion in the market, and to encourage widespread use of the new SCCs and reduce any risk of cost increases being passed on to EU businesses and consumers.

Clause 5: Description of the Transfer(s)

- **Clause 4 Hierarchy** – We recommend clarifying that the hierarchy provisions would not prevent the parties subsequently amending the Annexes, and that this provision only applies in respect of agreements "relating to the same subject matter." This would avoid any issues should the parties, in a different context, enter into a different data processing arrangement (e.g., C to P and C to C arrangements co-existing in respect of different data).

Clause 6: *Optional* - Docking Clause

- **Page 3 Clause 6.a** – We recommend clarification on how to formalise "agreement of the parties" for accession of a new party. The question here is whether all existing parties have to sign an accession agreement or whether it would be sufficient for the new party to complete and sign the annexes.
- **Page 3 Clause 6.b** – We recommend rephrasing the language so that upon accession, the new entity receives the rights and obligations of the data exporter/importer, and the other

parties simultaneously receive the relevant rights and obligations in respect of the new entity. One potential way is to replace "the acceding entity shall be treated as a Party to these Clauses" by "the acceding entity shall become a Party to these Clauses."

Section II: Obligations of the Parties

Clause 1 Data Protection Safeguards

- It should be clear that the provisions of Section II, Clause 1 are at all times subject to the provisions of Clauses 2 and 3. Otherwise, parties who comply with Clauses 2 and 3 may still find themselves in breach of Clause 1 (for example, the provisions regarding onward transfers, transparency and access).
- **Page 3 Module 1 Clause 1.1 Purpose** – We would appreciate the addition of suitable lawful basis in addition to the reference of consent. The SCCs shall consider all GDPR legal basis and not only consent. If the intended processing is not compatible with the options laid out in the SCCs (Annex I.B.), the SCCs should allow the data importer to use the appropriate GDPR legal basis (articles 6 or art. 9 GDPR, as applicable), which are not limited to consent. ITI noted that clause 1.1 requires data subject's consent for purposes that are incompatible with the specific purpose of the transfer, while clause 1.2 a (ii) refers to purposes that are different. The language should consistently refer to incompatible purposes. It should be specified that the importing processor or sub-processor need only comply with the lawful instructions of the exporting controller/processor (assessed by reference to EU law).
  Page 3 Module 1 Clause 1.2 Transparency – The transparency obligation goes beyond the requirements of GDPR and is not practicable. The GDPR requires only "categories of recipients" to be identified, but subparagraph (iii) requires the "identity of the third party". We note that in the controller-to-controller module, the transparency obligations are unclear and would encourage clarification towards viability of privacy notices in these scenarios. In particular, the SCCs should not modify the GDPR information duties. In particular, if onward transfers are foreseen, the categories of recipients must be addressed rather than the "identity of that third party."
- **Page 4 Module 1 Clause 1.5 Security of processing** – We recommend data breach language to align with the GDPR. The draft states "is likely to result in significant adverse effects," while the GDPR had a different definition of reportable breach as a breach that is likely to result in "risk to the rights and freedoms of natural persons."
- **Page 7 Module 2 Clause 1.3 Transparency –** We recommend making the obligation to provide data subjects with copies of the Clauses an obligation solely of the data controller. The data processor should only have an obligation to forward on a request to the controller.
- **Page 7 Module 2 Clause 1.4 Accuracy** – We recommend that the accuracy duties of each controller shall be independent. The obligation of the parties to keep the others updated of the accuracy of the data does not make sense in all instances where the data importer and the data exporter do not continue to process the same data for the same purposes. Further, the exporter should not process for their own purpose. In addition, this obligation cannot be indefinite. The data subject will have an independent relationship with each controller and shall be able to determine which data it continues sharing with each of them. An addition period of time for erasure or anonymization in back-up copies is always required in practice as well.

- **Page 7 Module 2 Clause 1.5 Storage limitation and erasure or return of data** – We recommend that the language reflect the GDPR options to return/destruction of the data upon termination. We encourage a broader wording regarding timing and available options in this section to allow for more flexibility regarding handling of data in such cases. For example, in addition to the deletion or return to the controller, the controller may determine that the processor sends the data to another processor appointed by the data controller. The data controller may also determine that part of the data is deleted and another part is returned to the data controller, directly or to another processor appointed by the data controller. We therefore recommend including an additional option, i.e., a prior notice agreed between the parties before the termination of the agreement. The controller shall determine the destination of the data, that may include the deletion and/or the return to the data controller, directly or to another processor appointed by the data controller. The parties may also agree to a regime by default if the controller fails to communicate its decision to the data processor in the agreed term. The parties shall also address the economic consequences of either option. We also recommend reflecting that the parties may need to maintain data for a time post termination or expiration of the agreement to permit the data exporter to move the data and validate the data prior to the data importer returning or destroying the data.
- **Page 7 Module 2 Clause 1.6 (a) Security of processing** – The provisions on pseudonymisation in this paragraph should be amended to acknowledge that, in many cases, 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 will not be the data exporter under Module 3) may be the entities that hold additional information about the user in order to re-identify them, such as an end user (i.e., data subject) ID number. As another example, neither the exporter processor nor the importer sub-processor will control the pseudonymisation where an industry standard technique (such as hashing) is used. The obligations in this sub-paragraph should therefore only apply to the extent applicable.
- **Page 8 Module 2 Clause 1.6(c) Security of processing** – We recommend clarifying whether the language "the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its adverse effects" is addressing steps the importer should take to understand the cause of the breach and to stop further losses of personal data. The mechanics of responding to a data breach should be the responsibility of the controller, which could also be negotiated by the controller to be the responsibility of the processor, so that there are no confusing communications by both parties to affected data subjects.
- **Page 8 Module 2 Clause 1.7 Special categories of personal data and 1.8 onward transfers**– We recommend clarifying the language on "onward transfers," specifically around third parties who will receive data having to agree to be bound by the clauses.
- **Page 9 Module 2 Clause 1.9(d) Documentation and compliance –** The current language mandates that "where the data importer mandates and audit for the data exporter, it has to bear the costs of the independent auditor." The SCCs should permit the parties to agree among themselves which approach they want to take under the three options provided. Further, requiring that audits also include inspections at the premises of the data rewrites the GDPR art. 28; instead, data processors outside of the EEA should be held to the same standard that applies to processors in the EEA. Also, inspections of data centers where global cloud services are hosted presents potential confidentiality and security risks for all other customers of the data importer. There should be a possibility for the parties to agree

on alternative approaches on how to assess data importers' compliance with the law and with the contract.

- **Page 9 Module 2 Clause 1.9(e) Documentation and compliance –** ITI recommends that the onus of responding to requests from the regulator is more appropriately for the data exporter who has the obligation to ensure that the data importer complies with the SCC requirements.
- **Page 9 Module 3 Clause 1.1 (a) Instructions –** It is not practicable or desirable for the processor to identify the controllers to the sub-processor. For large-scale commercial services, this list would permanently need updating. It will also represent confidential information of the exporting processor (effectively a 'client list'), which the sub-processor could then target directly, and will tend to increase data flows, transfers and usage rather than minimizing them. Finally, in many multi-party scenarios, the instructing party is likely, themselves, to be a processor (and Module 3 is being used in a sub, sub-sub, or even sub-sub-sub processing scenario). We note that Article 30(2) requires the processor to maintain this list internally, and only make it available to the SA (and only on request) may be difficult to implement in practice.
- **Page 9 Module 3 Clause 1.1 (b) Instructions –** The obligation requires data importers to accept instructions from both the data exporter and the controller will create a situation where a processor must accept instructions directly from a controller with whom the processor has no relationship. Requiring a sub-processor to respond to instructions from a controller they do not know and cannot verify upends the protections of that processor and creates security implications that could be disastrous. To maintain adequate security and privacy protections, data importers should only be required to accept instructions from the data exporter.
- **Page 10 Module 3 Clause 1.4 Accuracy –** This obligation is not imposed on processors under the GDPR, and it is unclear why it is necessary by virtue of the data leaving the EEA. It seems unlikely that processors would have sufficient context to understand whether data was inaccurate or out-of-date, and undesirable that they should have a role in monitoring this. We recommend this provision be deleted. By way of a comparison, we note the processor Bonding Corporate Rules (BCRs) address accuracy by imposing a duty on processors to execute any measures to update, correct or delete data, when asked by the controller- an obligation consistent with the processor's role.
- **Page 10 Module 3 Clause 1.6 (a) Security of processing –** It should be clarified what it meant by "in transmission," given the potentially varied interpretations of this term in a technical context. Given the realities of the data processing service industry, it is important to recognise that there will very often not be one act of "transfer" of data between party A and party B, but rather ongoing and instantaneous data flows between multiple service users, inherent to the nature of the services.
- **Page 11 Module 3 Clause 1.6 (c) Security of processing –**The specific requirements for the data breach notification go substantially beyond what is required of EU processors under the GDPR Article 33(2), and the assistance obligation under Article 28(3)(f) (which, we note, takes into account the nature of the processing and the information available to the processor). It is unclear why the existence of a data transfer should require these enhanced obligations. This obligation would be extremely challenging for importers to implement at scale and requires a subjective assessment by the processor as to the "likely consequences" of the breach and would likely require the processor to obtain detailed knowledge about the data it processes on behalf of the controller. This assessment is for the controller, and not the processor, to make. Given that SCCs are limited to transfers, we could limited to

comply with its obligations under Chapter V of the GDPR (and still subject to reasonableness) for all reasons outlined. Further, we recommend delayed notifications should be considered acceptable in some cases where the wider circumstances are justified. The notification provisions within Clause 3 could be enhanced through more consideration of countervailing interests such as public safety and benefits deriving from delayed notification. Even where notification is delayed due to exceptional circumstances or upon expiration of a non-disclosure period outlined in the legal process, it still affords data subjects the opportunity to exercise their rights. In a processor to processor (P2P) context, obligations for data importers to notify data subjects are only possible when the data importer has a direct relationship with the data subjects. We ask the Commission to consider broadening this provision to entities acting on behalf of the data controller.

- **Page 11 Module 3 Clause 1.6 (d) Security of processing –** The cooperation and assistance obligation on the importer in Clause 1.6(d) should be subject to a "reasonableness" condition, particularly given the breadth of this obligation ("in any way necessary to enable the data exporter to comply with its obligations under GDPR"). Importers should not have to expend unreasonable resources and provide services they would not otherwise provide (e.g., legal advice) or act substantially against their own interests. This would appear to go significantly beyond what is required of data processors under Article 28(3) or Article 33(2) of the GDPR.
- **Page 11 Module 3 Clause 1.7 Special categories of personal data –** The SCCs should not mandate specific restrictions and additional safeguards for special category data. In the majority of cases, we anticipate the presence of special category data would simply entail a higher standard of security being applied to all the data. Moreover, in many processor scenarios, there is no need (and it should not be encouraged) for the processor to know the nature of the data it processes (in keeping with the idea of 'least privilege').
- **Page 11 Module 3 Clause 1.8 Onward transfers** – It should be clear that the obligations in Clause 1.8 (onward transfers) are subject to the provisions of Clauses 2 and 3. Otherwise, a party may comply with Clauses 2 and 3 but still be in breach of Clause 1.7. One way of achieving this would be to ensure that the concept of "onward transfers" is narrowly defined to disclosures initiated by the data importer. This should exclude: (1) disclosures initiated by the data subject; (2) law enforcement disclosures which are subject to Clauses 2 and 3; and (3) unauthorised access (i.e., hacking). This comment is equally applicable to Modules 2 and 3.
- **Page 12 Module 4** – Overall, we recommend this Module be given greater thought, as we rarely consider it appropriate to use the same Module 1 wording in Module 4 (as is proposed in numerous cases). In some cases, this simply leads to confusion and inaccurate drafting (e.g., the reference to the importer's sub-processors in Section II, Clause 7). However, in many cases the effect is to undermine the controller-processor relationship, by giving an inappropriate level of discretion and authority to the processor. This will be particularly problematic for importing controllers who are themselves directly subject to a regulatory regime which includes controller/processor distinctions. As drafted, we think the SCCs would ultimately become a material disadvantage for EU service providers seeking to market their services to non-EU based customers, because of the risks and obligations which must be assumed by the customer. It also creates regulatory risk for the EU processor, who is obliged under art. 29 of the GDPR to only act on the instructions of the controller, but could be subject to a conflicting obligation under the SCCs (e.g., to refuse to return the data).

- **Page 12 Module 4 Clause 1.3 Documentation and Compliance** – We acknowledge that accountability is a key principle of the GDPR that must be reflected in the Clauses, and that record-keeping is essential to accountability, but if "the Parties shall be able to demonstrate compliance with these Clauses" is made a contractual term, this Clause will impose an over-broad obligation that, strictly speaking, neither party will ever be able to fulfil given the impossibility of proving a negative (for example, no party will ever be able to "demonstrate" that it hasn't processed any data in breach of the clauses). We are concerned that the inclusion of an impossible obligation, when combined with the data importer's obligation to inform the exporter if the importer is unable to comply with the Clauses, could serve to undermine the credibility of the Clauses, or prevent their use by conscientious actors. (This comment also applies to equivalent wording in Module 4.) Additionally, the importer should have the right to reasonably object to an auditor (for example, it would not be appropriate if a direct competitor of the importer were to be appointed by the exporter as its auditor) provided the exporter can then choose an alternative auditor. It would also be helpful to replicate the protections in the existing SCCs (and Processor BCRs), which require the auditor to be in possession of the required professional qualifications bound by a duty of confidentiality.

Clause 2: Local Laws

- **Page 13 Clause 2 (a)** – ITI recommends Clause 2(a) be explicitly linked to the assessment in Clause 2(b). As currently drafted, the two provisions potentially contradict each other, and parties will be reluctant to give the warranty in paragraph (a) if their risk assessment reveals supplementary measures are needed. Clause 2(a) should be amended so that it is clear that the parties' warranty in paragraph (a) takes in account the matters referenced in paragraph (b).
- **Page 13 Clause 2(b)** – ITI recommends adding clarification that neither party is under the obligation to provide legal advice to the other party by the requirement of the applicable Clause. Also, ITI recommends that the primary responsibility should be on the data exporter to determine whether the export meets legal requirements.
- **Page 13 Clause 2(c)**– We welcome the statement that the data importer has the role of cooperating with the data exporter but strongly urge that the EDPB recommendation and SCCs be aligned to confirm that the data exporter has the primary responsibility to carry out the assessment.
- **Page 14 Clause 2(d)** – The data exporter should create and maintain the documentation.
- **Page 14 Clause 2(f)** – It should be clarified that the exporter can only mandate "appropriate measures" which can reasonably/practically be implemented by the importer. This provision cannot be a 'carte blanche' for the exporter to require any changes to the processing, no matter how impractical or expensive. It should be made clearer in which scenarios a data exporter is obliged to inform the competent supervisory authority of data transfers when applying additional safeguards, and in which cases doing so is merely optional. The *Schrems II* case ruling indicates that consultation with the authority is recommended when the data exporter has reason to believe that the data importer cannot fulfill its obligations even if supplementary measures are used. The right to terminate the contract should only apply to the specific element(s) relevant to the SCCs. Data transfers will often form part of a much wider provision of services, and this right should not enable clients to terminate an entire framework, of which the data processing services may only form a discrete and severable aspect.

Clause 3: Government Access Request Obligations for Data Importers

- **Page 14 Clause 3** – We recommend adding a definition of 'public authority' to confirm that this concept relates to law enforcement authorities. This clause should be limited to requests that are broad or indiscriminate from law enforcement authorities (or similar agencies). 'Law enforcement authorities' was the phrase used in the previous SCCs and is the focus of *Schrems II*. Additionally, the trigger for the government access request for these Clauses is not sufficiently clear. Would this include data collected directly from EU users by a platform provided by the processor, as part of the services? Do the data subjects need to be in the EU, or would it include any data collected worldwide by an EU processor? It should also be clarified that, where Clauses 2 and 3 are triggered, they will only apply in respect of the personal data collected by the processor in the EU. In other words, these Clauses should not have a 'contagious effect' and attach to all personal data processed on behalf of the controller.
- **Page 15 Clause 3.1 (c) (d) & 3.2** – The obligation "to exhaust all available remedies to challenge the request" is not practicable, when considered in the context of a normal commercial relationship. This potentially implies a requirement to pursue all lines of appeal, for example, irrespective of the time and resources required, or the prospects of success. In many cases this would simply not be productive. The same concerns apply as regards: (1) the obligation to seek interim measures; and (2) the obligation to use "best efforts" to obtain a waiver of the notification obligation under Clause 3.2(b) (best efforts being usually interpreted as a very high standard of obligation). This language is particularly problematic in a Controller to Controller context, or Processor to Controller context, where the importer is processing the data for its own benefit and must exercise its own discretion. We recommend this language be updated to either ask the data exporters to provide a summary of requests (in cases where it's not possible to share the precise details of the specific request due to legal restrictions) or reword the requirement from 'agree to provide' information on requests to 'agrees to make available on request.' Also, requiring challenge in each case seems overly prescriptive. And what would a challenge look like it, particularly if an organization determines it has an obligation to comply? We recommend revising the obligations imposed directly on data importers.

Clause 4 Use of Sub-Processors

- **Page 16 Module 2 Clause 4 (a)** – Despite the headings, the drafting essentially removes any distinction between prior specific and general written consent to sub-processing, the two distinct types of sub-processor authorisation clearly provided for by Article 28(2) of the GDPR. Since Option 2 (General authorisation) requires a list of sub-processors to be included in Annex III, it is difficult to see how this is distinct from a specific consent to those organisations listed (Option 1). It should also be clearer that sub-processors who are listed in Annex III when the Clauses are entered are permitted to start processing data immediately. The current drafting does not exempt them from the requirement for specific authorisation to be requested a certain number of days ahead of time.
- **Page 16 Module 2 Clause 4 (b) & Page 17 Module 3 (b)** – Where a data importer engages a sub-processor to carry out activities on behalf of the data exporter, clarification is

requested. For example, whether a separate processor to sub-processor agreement can be signed with the "same" obligations (similar to current flow-down) or whether the sub-processor has to somehow sign on to the controller-processor agreement?

- **Page 16 Module 2 Clause 4 (c) / Page 17 Module 3 (c)** – It should be confirmed that only the flowed-down data processing provisions need to be provided, and so the processor can remove any confidential or commercial terms. We recommend adding a statement here outlining that commercial terms can be redacted.
- **Page 16 Module 2 Clause 4 (e)** – It should be clarified that the sub-processing agreement does not need to continue but that, in the event of termination, the data exporter can benefit from any rights accrued prior to termination. In practice, an insolvency event would often terminate the agreement, and it should be clear that the controller cannot compel the ongoing commercial sub-processing arrangement to continue.

Clause 5: Data Subject Rights

- **Page 17 Module 1 Clause 5** – ITI recommends clarify the obligations of the data exporter and whether the two parties must assist each other in responding to requests, including whether the data subject must make requests separately or to only one of the controllers. In addition, permit the parties to contractually agree how to handle data subject requests between the two controllers, which may result in a more comprehensive and easier interface for affected data subjects.
- **Page 19 Module 3 Clause 5 (a)** – The data importers shall notify data controllers, where appropriate, about the data subjects' requests. We recommend clarification on criteria for determining when it is considered appropriate for data importers to notify controllers.

Clauses 6 Redress, 7 Liability, and 8 Indemnification

- **Page 20 Clause 6, 7 and 8** – Only data importers which are data controllers (and not data processors) are under the duty to provide information of where to address complaints to the data subjects. Further, only tangible, real and evidenced damages for an individual should be enforced and compensated in a court (and not theoretical, merely claimed or unevidenced claims). We would welcome additional guidance in the draft SCCs on the possibility for parties to manage liability and indemnification commercially between them (without prejudice to data subjects).

Clause 9 Supervision

- **Page 21 Clause 9 (b)** – The importer's acceptance of the jurisdiction of the competent SA should be subject to the GDPR's rules on SA competence, including the One-Stop-Shop (OSS), to avoid any potential conflicts as to which SA has jurisdiction over a particular transfer (and/or to avoid parties being subject to overlapping enforcement contrary to the principle of non bis in idem (a party should not be penalised twice for the same wrong). ITI recommends that the data importer only be subject to audit to resolve a complaint or other matter, and that the audit right does not apply at all times.

Section III Final Provisions

Clause 1 Non-compliance with the Clauses and Termination

- **Page 22 Clauses 1 (b) & (d)** – The provisions here are not contingent on the processor having collected the data in the EU. Clause 1(b), by requiring the processor to suspend the transfer, essentially requires the processor to hold the data hostage, in direct conflict with the Processor/Controller relationship. Additionally, the most concerning language is the deletion obligation in Clause 1(d), which would require a controller to delete its own data (which could, for example, relate to its own employees or customers). As above, these obligations would place EU service providers at a clear disadvantage in the international market. The SCCs should not provide for the return or deletion of all data on termination, as in many cases the issue of non-compliance may only apply to a particular piece or sub-set of data. The relationship between the two controllers may be long-standing and have involved significant commercial investment by the importer.
- **Page 22 Clause 1(c)** – Under the previous clauses the data exporters had the option of suspending the transfer of data or terminate the contract. In the current draft, the only option is to terminate the contract. The option of suspending the transfer should be reinstated. The decision to suspend a personal data transfer shall be a balanced and harmonised approach. We also recommend a more specific approach to notification processes for supervisory authorities so as not to lead to excessive requirements.

Clause 2 Governing Law Clause

- **Page 23 Clause 2** – There is a lack of clarity of the choice of governing law when third-party beneficiary rights are invalid or OSS does not apply. When the data exporter's law does not recognise third party beneficiary rights, it is unclear which governing law should apply for and, in any event, the solution proposed will create a conflict of law (a German Court applying Estonian contractual law to a German entity?) When the data exporter is not eligible for the OSS, it is unclear which governing laws and jurisdiction it may apply for.