AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

AmCham EU input to the public consultation on the revised set of Standard Contractual Clauses for transferring personal data to non-EU countries

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and U.S. positions on business matters. Aggregate U.S. investment in Europe totalled more than €3 trillion in 2019, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

AmCham EU welcomes the update of the Standard Contractual Clauses (SCCs) by the European Commission. These clauses are an essential and efficient tool to enable organizations to transfer personal data from the European Union to third countries . We strongly welcome the effort the Commission has put into developing new SCCs that are pragmatic, flexible and update data subjects' rights in accordance with the General Data Protection Regulation (GDPR). The revised SCCs represent significant effort to modernise and update the instrument as well as filling the legal limbo left by the recent Schrems II ruling hence reducing the level of legal uncertainty thereof and the consequent operational difficulties for European businesses. The long-term solution to the challenges raised by the ruling will need a political solution. These SCCs are a welcome step towards legal direction but now more than ever it is important for the EU and the US to come together and reinvigorate the transatlantic relationship.

Risk-based approach

AmCham EU fully support the Commission's efforts to ensure that SCCs (Paragraph 20 of the implementation decisions and clause 2 of the annex) retain the risk-based approach to international transfer found within the GDPR. SCCs and other GDPR transfer mechanisms are crucial tools for organisations to benefit from the digital economy and society in a safe and secure manner. These SCCs are a pragmatic recognition of the importance of factual circumstances and individual context of data transfers that need to be considered in order to assess the relevant specific risks on the ground and in practice. This is consistent with the GDPR and the Court of Justice of the European Union (CJEU) which are focused on protecting against the actual possibility of damage and risk, as opposed to theoretical possibilities. We encourage the Commission to continue building on this approach in the final version. This can be assisted by including direct references to the accountability principle of the GDPR. The risk-based approach is equally important as it prevents unrealistic or misleading expectations being placed on organizations for factors outside their control. We would especially welcome clarification as to whether the entire transfer risk assessment is required for any and each transfer (regardless of risk). If it is clear that the transfer poses no risk to the individual (because very limited data), the transfer risk assessment imposes onerous burdens and paperwork on the parties and should not be required (in full).

Remediation of contracts

Article 6 of the draft Implementing Decision requires the replacement of the existing SCCs within one year from the date of entry into force of the Decision. Considering that the current SCCs have been used for almost two decades by thousands of stakeholders, providing a deep level of protection and safeguard substantially similar to the new SCCs, and that parties are already required to verify if additional measures should be in place following EU Court decision (Case C-311/18), the request to update all the contracts appears not necessary and extremely burdensome. Especially, now that companies have had to implement the GDPR, and update all their contracts after the invalidation of the privacy shield and/or to prepare for a hard Brexit during the past year(s). It would be best to allow exporters and importers to benefit from a longer transition period for **existing contracts** and to apply the above one year period **only for the new contracts**. This will also be in line with the Commission instruction of the previous (controller to processor) SCCs update back in 2010. Alternatively, it would be helpful and save a lot of paperwork if the Commission would consider the current SCC to be automatically replaced by the new SCC (taking into account the role of each party), whereby parties will obviously still be required to undertake transfer impact assessments and implement supplementary measures.

Timeline

The Commission has provided organisations with a one-year transition period to implement the new SCCs, after which time the current SCCs can no longer be relied on to legitimise transfers. This proposed transition period is very short and is likely to pose significant challenges for many businesses, especially multinational companies that may have hundreds or even thousands of contracts that incorporate the current SCCs. This is particularly so given that the new SCCs require companies to document their assessments of the data transfers, taking into account the specific circumstances of the transfer, the laws of the third country of destination, and any safeguards adopted in addition to the SCCs (Section II, Clauses 2(b) and (d)), all of which could take a significant

amount of time to document. A two-year implementation period would be more appropriate in this respect, similar to the implementation period that the GDPR provided.

'All available remedies' to challenge a request for disclosure

Under the new SCCs, the data importer has the obligation to exhaust all available remedies to challenge a request for disclosure if there are grounds to do so. Exhausting all legal remedies may be impractical and too onerous. Instead it would be more appropriate, in line with the risk-based approach of the GDPR, to allow the data importer together with the data exporter, where it can be informed of the request, to assess the exposure for the data subjects and determine the appropriate course of action (eg, injunctive relief). In that assessment, it is paramount to determine whether a recourse has a suspensive effect as otherwise the disclosure would be required anyway pending its resolution.

Local laws affecting compliance with the Clauses

Clause 2, Section 2 imposes specific obligations on the data exporter and importer with respect to the assessment of the laws of the 3rd country, following Schrems II. If the importer is required to notify the supervisory authorities, whether the data transfers will continue or be suspended following changes in local legislation without any distinction, this will likely result in an unmanageable flood of notifications for the supervisory authority. Instead, notification after the termination of a contract provides a filter that allows possible inappropriate behaviour to be flagged, allowing the authorities to investigate the importer's arrangements with other exporters.

Obligations of the data importer in case of government access requests

Clause 3, Section 2 extends the notification requirements relating to government access requests and requirements to review the legality and challenge requests. In our view, the obligation should be for the importer to notify the exporter in case of government access requests. It then should be determined by the exporter to inform the data subject, as deemed appropriate. In order to present information in a consumable form, including in published transparency reports, the obligation should be to make relevant information available, instead of the greatest amount possible.

'Direct interaction importing processor and controller'

The SCCs require direct interaction between sub processor – controller (in the context of transfer processor – processor). The data importer must provide notices and assistance to the controller. Furthermore, if the importing processor wants to engage sub-processors, it must provide notice to the controller. This should be managed by the exporting processor rather than by the importing processor. The exporting processor is the one that entered into a data processing agreement with the controller and should act as the point of contact. If not, the controller could be contacted by an importing processor (with whom it does not have a direct relationship) which will only create confusion, extra work, time and money (finding out which contract this sees to etc.), and duplication of work (as the importing processor will also inform the exporting processor that will in turn be under an obligation to inform the controller as well). We would welcome the Commission to reassess this.

Clarity Needed

In addition, there are a few elements, for which we would welcome further clarity:

1. **Additional safeguards:** The SCCs include a specific reference to 'additional safeguards' (a notion introduced in Schrems II) that may be required to ensure adequate protection of personal data imported from the EU to a third country. Clarity around what those safeguards might be will depend on the final guidance from the European Data Protection Board (EDPB);

2. **Docking clause:** It is unclear as to whether Section I - Clause 6 is always Optional or if there are any cases in which it is mandatory to include it. If the latter, we would then welcome clarity on which cases such Clause is mandatory. In addition, the mechanism by which new parties can join is not clear. The SCC say that the new party may accede by completing a new data transfer Annex, "by agreement of the Parties". Please clarify whether parties are free to decide how to give "agreement", e.g. prior, general agreement, by separate documents;

3. **Parties of module 2:** We would also welcome further clarity on whether module 2 is required only when there is a direct contractual relationship between the controller and the processor, and therefore in case of sub-processor established in a third country, only the module three 'processor to processor' should apply;

4. **GDPR article 3(2)**: The SCCs in their Annex provide appropriate safeguards within the meaning of article 46(1) and (2)(c) of GDPR for the transfer of personal data from a controller or processor subject to GDPR (data exporter) to a controller or (sub-) processor not subject to GDPR (data importer). The provisions above could suggest the draft SCCs should be used only when the 'data importer' is not directly subject to the GDPR itself. Further clarity would be welcomed regarding if data transfer mechanisms may not be needed when personal data is transferred to a company outside of the EU that is already subject to the GDPR under article 3(2);

5. **Annex I - list of parties - controllers:** It is unclear if for module 3, the list of controller(s) will be necessary only if they join the Clauses as additional parties via the Docking clause. If this is the case, we would call on the Commission to make it clearer that otherwise this section is not necessary. We note that if it would be mandatory to add controllers as an executing party for Module 3, this would in our view defeat the purpose of SCC for processors – processors and create a lot of extra paperwork for the parties.

6. **Liability caps between parties:** Please inform what happens if the data processing agreement / main agreement in place between parties has privacy liability caps– would that be conflicting with the SCC or can that be complementary? We would call on the Commission to specifically refer to potentially agreed liability caps between the parties.

7. **The data breach reporting requirement for non EEA controllers refers to "significant adverse effects".** We would call on the Commission to align this with article 34 GDPR to avoid confusion.

8. **Modular approach**: While it is welcome that the Commission provides for a wider range of processing scenarios than before, the use of the modular approach with bracketed language is impractical and, when adopting the SCCs in final form, clean drafts for each processing scenario should be published. This will provide certainty to data exporters and data importers as to the complete set of contractual provisions in SCCs that will enable such parties to satisfy their obligations under the GDPR.

9. **Sufficiency**: With respect to the sufficiency of the SCCs to provide certainty regarding the validity of data transfers to third countries, it is critical that companies can rely on the SCCs as approved by the Commission, without the risk that DPAs seek to impose additional requirements beyond the SCCs. Accordingly, the Commission should make a clear statement in its implementing decision that:
    - the use of the modernised SCCs precludes DPAs from requiring additional clauses for transfers to third countries; and
    - that such SCCs may be used for transfers to any data importer in any third country.