insurance
europe

Position Paper

Comments on the development of Q&As on Standard Contractual Clauses on transfers of personal data to third countries

Our reference:	COB-DAT-21-066	Date:	November 2021
Contact person:	Danilo Gattullo, policy advisor conduct of business	E-mail:	gattullo@insuranceeurope.eu
Pages:	5	Transparency Register ID no.:	33213703459-54

Insurance Europe welcomes the opportunity to provide input to the European Commission (EC) on the development of a questions and answers (Q&As) document on the new Standard Contractual Clauses (SCCs) on transfers of personal data to third countries.

Insurance Europe supports the EC's approach with respect to the SCCs on data transfers to third countries and, in particular, the acknowledgment that companies should be able to take into account the specific circumstances of data transfers and their own "documented practical experience" when assessing whether the SCCs provide appropriate safeguards.

Nevertheless, European companies face severe challenges in judging the legal requirements of third countries. Rather than investing in a multitude of global law firms providing expertise in each jurisdiction, it should be for the national data protection authorities to determine whether the local laws and customs of a third country represent an obstacle to the transfer of personal data to that country. At a minimum, the EC or the European Data Protection Board (EDPB) should make publicly available trustworthy resources on the relevant legislation of the EU's main trading partners.

The upcoming Q&As should address practical questions that EU businesses may have when adopting the new SCCs. To this extend, Insurance Europe recommends that the Q&As address the questions below.

Potential questions that can be addressed by the Q&As

General comments

As a general principle, to ensure the proper application of the SCCs, the Q&As should address the new features introduced by the clauses, such as:

- The SCCs modular approach.
- The introduction of a docking clause allowing new parties to accede to the international data transfer agreement between the existing parties.
- New responsibilities and obligations for the data exporter and data importer.

- The Q&As could also contain or redirect to examples of additional technical, contractual, and organisational measures (eg transparency measures).

It is also important to ensure that EU companies can continue to rely on common businesses tools, such as cloud computing. In this regard, the Q&As should provide practical examples on the applicability of the SCCs with third country cloud providers: For example, if a data controller hosts its data in the cloud in Europe, but the cloud provider is a subsidiary of a third country company, should SCCs be integrated in the contract with the EU subsidiary of the third country company in Europe?

General questions

Question: *It is indicated that the standard contract clauses may be annexed to a larger contract. In this case, do they need to be completed and signed, or is a simple reference to them with a single signature in the contract possible? In other words, can one simply indicate adherence to the Commission's model with a simple reference to the text?*

Comments: Companies should be able to incorporate by reference the new SCCs in the existing contract, provided that they specify the modules that suit the relevant relationship (eg controller to processor). Companies could simply add a clause to the agreement stating that the parties agree to and incorporate in their entirety the new SCCs with the relevant modules so that the new SCCs do not have to be restated in their entirety in the document.

Question: *The new - optional - docking clause, Clause 7, allows third parties to join existing standard contractual clauses without having to conclude separate contracts parties. In practice, how does this happen? Is it necessary to have the third-party sign or is a simple adherence to the annexed clauses sufficient?*

Comments: The new SCCs say that: An entity that is not a party to these clauses may, with the agreement of the parties, accede to these clauses at any time, either as a data exporter or as a data importer, by completing the appendix [which describes the parties] and signing annex I.A. Therefore, it should be possible to add a single signature page that can be easily updated and signed by the parties whenever a new party joins. However, parties still need to set out the procedure for how this will work in practice.

Question: *Can the non-applicable Clauses/Modules enumerated in Clause 3 ("Third-party beneficiaries") be deleted in spite of the statement in Clause 2 (a) according to which the SCCs shall not be modified except "to select the appropriate Module"?*

Comments: The SCCs should follow a modular approach. Data exporters can tailor the SCCs to the specifics of the data transfer in question by choosing the suitable module(s). According to Clause 2 (a), the SCCs only set out appropriate safeguards pursuant to Article 46 of the General Data Protection Regulation (GDPR) provided they are not modified, except to select the appropriate module(s) or to add or update information. Meanwhile, Clause 3 enumerates all Clauses which may be invoked and enforced by data subjects as third-party beneficiaries. Unlike, for example Clause 8, the applicable modules cannot be selected in Clause 3. Rather, the non-applicable Clauses/Modules can only be deleted. This, however, may go against the wording of Clause 2 (a), since Clause 3 would be modified. On the other hand, leaving Clause 3 as is would lead to discrepancies, misunderstandings and legal uncertainty for the data subjects if Clause 3 refers to Clauses and modules that are not applicable and have therefore not become part of the SCCs in the specific case. For these reasons, it should be possible to remove the non-applicable Clauses from the list in Clause 3.

Territorial scope & applicability

Question: *Can Modules 1, 2 and 3 of the SCCs be used if the data exporter is established outside of the EU/EEA?*

Comments: Publications on the updated SCCs exclusively refer to the transfer of personal data to third countries by "a controller or processor established in the EU/EEA". This has led to many companies becoming unsure about whether these modules can be used if the data exporter is not established in the EU/EEA. While the respective modules will, in most cases, be used by data exporters established in the EU/EEA, the SCCs themselves do not make a distinction based on the data exporters country of establishment. Instead, the data exporter is defined in Clause 1 (b) (i) as "the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data". Furthermore, sentence 2 of Recital 7 of the EC implementing decision on the SCCs also assumes that the modules can be used by controllers and processors not established in the EU.

This question is especially important with regard to the applicability of Module 3 (transfer processor to processor), if a controller in the EU transfers personal data to a processor established in a third country subject to an adequacy decision, who in turn transfers the data to a (sub-) processor established in a third country without an adequacy decision. In such cases, it should be possible and sufficient if only the processor and the subprocessor conclude Module 3 of the SCCs. It should especially not be necessary for the controller to join the SCCs. The same should apply if the controller transfers the data to the initial processor on the basis of other instruments pursuant to Article 46 of the GDPR.

Question: *Does Module 4 of the SCCs (Transfer processor to controller) imply that its use or the use of other instruments pursuant to Article 46of the GDPR is obligatory in the following case? A third-country controller who is not subject to Article 3 of the GDPR transfers personal data not related to a person in the Union to a processor established in the EU/EEA. The processor only processes and transfers back the personal data that has been received from the third-country controller without combining it with personal data collected by the processor in the EU.*

Comments: Use of Module 4 or other instruments pursuant to Article 46 of the GDPR should be only voluntary in these cases. Module 4 of the SCCs should only apply if the third-country controller is subject to Article 3 of the GDPR with regard to the personal data transferred to the processor or if the processor combines the data received with other personal data collected in the EU.

Article 44 of the GDPR does not apply in the situation described with regard to the transfer of the personal data from the processor to the third country-controller. If the processor merely processes and transfers back personal data that has been received from the third-country controller without combining that data with personal data collected by the processor themself, the processor does not disclose any "new" data to a "new" recipient. The processor merely returns the data to the country that is their place of origin. As such, no increased risk arises from the transfer of the data back to the "third country".

In these cases, the requirement to use the SCCs for the transfer back would expand obligations resulting from the GDPR to data processing that does not even fall under the GDPR's territorial scope of application in the first place.

Question: *How shall sentence 2 of Recital 7 of the EC's implementing decision on the SCCs, according to which the SCCs may only be used to the extent that the processing by the importer does not fall within the scope of the GDPR, be interpreted? Does it mean that data exporters cannot conclude the SCCs with* *companies in third countries who also offer their services directly to data subjects in the EU since these companies would already be subject to Article 3 (2) of the GDPR?*

Comments: Recital 7 of the implementing decision should not prevent data exporters from using the SCCs with data importers who are subject to the GDPR by virtue of their other data processing. Sentence 2 of Recital 7 is only meant to refer to cases wherein the law is still inconclusive on whether a data processing has to be considered a "data transfer" (to a third country) pursuant to Article 44 of the GDPR. This encompasses cases in which the data exporter and the "data importer" are not separate legal entities: eg if the data exporter is a company and the data importer is merely one of its employees who processes the personal data in a third country. In these cases, the data importer is neither controller nor processor. It even remains undecided whether the data importer could be considered a "recipient" in accordance with Article 4 (9) of the GDPR.

The wording in sentence 2 of Recital 7 is highly ambiguous and has therefore caused much confusion. Since the relationship between Article 3 of the GDPR and Chapter V of the GDPR remains unclear, it is very likely that the EC only meant to exclude situations like the ones described above, wherein the existence of a "data transfer" in accordance with Article 44 of the GDPR is still legally unclear, and is expecting the EDPB to specify the relationship. The Q&A should explain this more clearly. Otherwise, the SCCs' scope of application may be understood to be much narrower to many users than what the EC originally intended.

Third country assessment and risk-based approach

Question: *Does the risk-based approach as outlined in Articles 24, 25 and 32 of the GDPR also apply with respect to the supplementary safeguards mentioned in Clause 14 (b) (iii) of the SCCs ("Local laws and practices affecting Compliance with these Clauses")?*

Comments: A risk-based approach should also apply when choosing supplementary safeguards that shall prevent access by public authorities on the basis of laws and practices in the third country of destination which prevent the data importer from fulfilling their obligations under the SCCs. This means that, depending on factors like the likelihood of data access by public authorities, the categories of personal data and the extent of the data processing a transfer of personal data to a third country without adequacy decision may still be performed even if the supplementary safeguards do not fully prevent the data access, but reduce the probability to a reasonably low amount.

The risk-based approach is a fundamental pillar of the GDPR that applies to all processing of personal data. It must therefore also apply to data transfers to third countries. The risk-based approach is expressed in particular in the selection of technical and organisational measures under Articles 24 and 32 of the GDPR. The implementation of the Schrems II legislation is concerned precisely with technical and organisational protective measures to prevent access by authorities in third countries. When assessing whether an equivalent level of data protection can be ensured, the risk-based approach must necessarily factor into the equation. If it is not applied to data processing in third countries, the EU would in conclusion demand a level of data protection from other countries that goes beyond the one guaranteed by the GDPR. However, several data protection supervisory authorities ignore the risk-based approach and require supplementary safeguards that completely rule out any possibility of data access by public authorities regardless of the specific circumstances of the data transfer. There is an overwhelming need for the EC's Q&A to answer this question definitively.

Technical and organizational measures (TOMs) to ensure the security of the data

Question: *Under Module 1 (transfer controller to controller), does the data exporter have to stipulate the data importer's TOMs similarly to how a controller determines a processor's TOMs in accordance with Article 28 of GDPR?*

Comments: Under Module 1 the data exporter should not be required to stipulate the data importer's technical and organizational measures.

Annex II of the SCCs (Technical and organizational measures including technical and organizational measures to ensure the security of the data) counts Module 1 among the transfer situations for which the data importer's TOMs must be specifically described. Among others, this has been interpreted as requiring the data exporter to stipulate the data importer's TOMs as if the data importer were a processor. The Q&A should clarify that this is not the case since such a requirement would contradict the differentiation between controllers and processors outlined in the GDPR. For comparison, concerning subprocessors the SCCs rightly do not provide for the use of Clause 9 with regard to Module 1.

Insurance Europe is the European insurance and reinsurance federation. Through its 37 member bodies — the national insurance associations — it represents all types and sizes of insurance and reinsurance undertakings. Insurance Europe, which is based in Brussels, represents undertakings that account for around 95% of total European premium income. Insurance makes a major contribution to Europe's economic growth and development. European insurers pay out almost €1 000bn annually — or €2.7bn a day — in claims, directly employ nearly 950 000 people and invest over €10.4trn in the economy.