Position Paper

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

09.12. 2020

Introduction

We welcome the European Commission public consultation period on Draft implementing decision and its Annex to discuss the standard contractual clauses (SCCs) for transferring personal data to non-EU countries as this is an important issue and an opportunity for stakeholders across all industries to provide input. In our view it was necessary to re-draft the SCCs to align them with the General Data Protection Regulation (GDPR). We would, however, like to point out some concerns and make suggestions to contribute to the public consultation which we believe the European Commission should take into consideration. For further elaborations and to go into more detail regarding the specific provisions, we are available at any time.

We appreciate the chance to provide comments on the new standard data protection clauses for the transfer of personal data to third countries pursuant to Article 46 GDPR. We acknowledge the great value of the updated framework, which will help companies when relying on third country transfers and value the efforts undertaken by the European Commission in modernizing the framework, also to reflect the Schrems II judgment. In particular, we welcome the introduction of the new Clauses also for the processor-to-processor environment.

From our perspective, there are several provisions and which can be further improved, such as related to terminology used, questions of enforceability and some provisions that seem to be phrased ambivalent. We also noted that some concepts may be subject to different interpretations or even misunderstanding by the parties actually implementing the Clauses.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Key Aspects

1. General Remarks

1.1. Transition Period

Most importantly, we would like to stress the point that the transitional period for the new SCCs (12 months) should not mean that all currently implemented SCCs should be amended and changed into using the new SCCs but rather that all SCCs that are already in place and working will continue to apply after the transitional period. In our view, it would suffice, fit the purpose and satisfy all interests if all contracts that are concluded after the transitional period will need to include the new SCCs. The existing contracts should enjoy a valid right of protection and continuity.

Remediation of contracts: Article 5 (implicitly) requires to replace the existing standard contractual clauses after the transition period or prior to it in case of relevant changes to the contract. Considering that the actual standard contractual clauses have been used for a decade in thousands of contract, providing a deep level of protection and safeguard substantially similar to the new clauses, 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. It will still satisfy the aim to secure transfer of data to third countries, if exporter and importer are required to apply them only for the new contracts when the SCCs will come effective. This will also be in line with the Commission instruction of the previous standard clauses update.

There is no need to replace the "old" SCC with the new version within a one-year period. The CJEU clearly stated in Schrems II that the previous SCC can still be used as the basis for a data transfer to a third country. An obligatory exchange of the previous SCC thus only leads to an enormous effort on the part of the companies. In addition, there is a concrete fear that this exchange will not be completed within the one-year period. A period of 12 months for updating existing SCC contractual relationships is too short. 24 months would be more appropriate and reasonably realistic.

One of the main reasons for the need for clarification is that many obligations under the new SCC will not be imposed on one party, but on both parties. In these cases, however, the parties will have to agree in advance on who will actually have to perform the task (see below for concrete examples). In addition, it is to be feared that (unless there are corresponding changes to the new SCC) many of the efforts made by companies with regard to the implementation of the GDPR will be wasted or will have to be taken on again in order

to comply with the new SCC (e.g. subcontractor lists, see below). A further reason is of course all the questions to be clarified in advance regarding the level of data protection in the third country concerned.

1.2. Setup and numbering of the Document

We appreciate the European Commission's approach to provide Standard Data Protection Clauses for four different international data transfers scenarios, and to offer certain optional clauses. We would like to respectfully submit that four separate documents, each addressing one specific data transfer situation, would be significantly easier to work with in practice.

In any event, we urge the European Commission to change the numbering of the document to a simpler and more intuitive format. We consider the current numbering scheme to be too complex, which will lead to substantial difficulties when working with the new SCCs in practice.

We suggest changing the general setup of the new Standard Data Protection Clauses, so that all determinations and choices to be made by the parties, such as choosing optional clauses, identifying supervisory authorities and/or applicable laws, are to be made in the Annexes of the new Standard Data Protection Clauses and not in the body of the actual Standard Contractual Clauses. This would greatly reduce the risk of accidental omissions in practice.

1.3. Practical implications of the new SCCs, unclear wording

Compared to the previous SCC, the new SCC appear to be considerably more stringent and far less practical than the previous SCC. On the one hand, there is an effort to fill the gaps in the GDPR and to comply with the Schrems II judgement, but the new SCCs overshoot the mark and disproportionately complicate the transfer to third countries. Moreover, many of the new clauses appear to be not very practical.

Overall, there is too much replication of the same wording across the Modules, without sufficient consideration of the specific scenario in question. For example, the same Annexes cannot apply for all Modules, since Annex III is not applicable to Modules 1 and 4, and Annex II is never mentioned (i.e. incorporated) in Module 4. The lack of proper consideration across the Modules is particularly problematic in Module 4 (which replicates much of Module 1), but equally applies as between Modules 2 and 3, and between 1 and 2. We suggest the Commission review each of the Modules, in detail, to determine whether any further amendments are needed to reflect the use case of that specific Module.

There are numerous examples of redundant drafting within individual Modules, and individual sentences. For example, in Module 2, Section II, Clause 1.1(b) would oblige the data importer to inform the exporter if the importer is unable to follow the instructions given to it, but Section III, Clause 1(a) already obliges the importer to inform the exporter if the importer is unable to comply with the Clauses. As a further example, in other places, the phrase "strictly necessary" is used even though "necessary" means the same thing.

1.4. Clarifications needed

The Commission should 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, subprocessor), or both. This clarity is essential, as it is currently unclear whether the controller can (or even should?) be a party to Module 3. Where the processor conducts the transfer (i.e. is the exporter) we assume there is no need (or basis) for the controller to be a party. In all cases, the controller signature block in Annex I of Module 3 should be deleted.

2. Section I – Clause 6: Docking Clause (page 3)

The introduction of the so-called 'docking clause' raises questions as it leaves many aspects unclear.

We would welcome clarity especially regarding whether this clause is optional or mandatory. Whilst the title clearly states optional, especially Section II Clause 1 Module 3 1.1 a seems to lean more toward making the clause mandatory. To our understanding of the provisions related to the processor to processor environment, the docking clause will be mandatory if provided conditions are met.

Furthermore, the intent of the docking clause is not yet clear and we would like to suggest adding explanatory remarks to the new clause.

Section II – Obligations of the Parties

3.1. Module One: Transfer Controller to Controller

3.1.1. Transparency (1.2. | page 3)

The transparency obligation as regards third party recipients in our view goes beyond the requirements of GDPR and is not practicable. The duty to inform the data subject would mean that contact data would have to be collected, although they may not be necessary for the actual data processing. The meaningful summary and SCC would probably also have to be translated into the data subject's native language. The GDPR requires only "categories of recipients" to be identified, but subparagraph (iii) requires the "identity of the third party". There is no basis for a higher standard than GDPR to be applied to the importer. It should also be clarified that this is subject to Clauses 2 and 3, and so the identity of law enforcement or public authorities do not need to be specifically disclosed as "third party recipients".

3.1.2. Onward Transfer (1.7 | page 5)

We would welcome clarification whether "agrees to be bound by these clauses" means joining the existing SCC, or means the conclusion of own SCC between the importer and further recipients. It should be clear that the obligations in Section II, Clause 1.7 (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.

3.2. Module Two: Transfer controller to processor

3.2.1. Parties and general scope

Parties of Module two: we would also welcome further clarity on whether module two is required only when there is a direct contractual relationship (DPA) between the controller and the processor, and therefore in case of subprocessor established in a third country, only the module three "processor to processor" should apply.

As a general comment, we see no basis for imposing additional obligations on processors or subprocessors, under the SCCs, which go beyond those imposed on processors under the GDPR, except to counter specific risks posed by the transfer (e.g. law enforcement access). Consequently, the 'general' Data Protection Safeguards in Clause 1 should mirror the obligations imposed on processors under the GDPR (directly) and under Article 28. They should not expand those obligations.

3.2.2. Instructions (1.1. | page 6)

The paragraph on instructions does not take into account the topic of remuneration for the execution of an instruction.

However, if the parties now insert their own remuneration regulations, there is a risk that these will be regarded as null and void because they could restrict the Data Exporter's right to issue instructions in that it does not issue instructions because they involve costs.

Since instructions can also always represent substantial change requests that are associated with massive costs, the importer has a justified interest in demanding a fee for instructions if they exceed the agreed scope of services. It therefore appears desirable to clarify that the parties can agree on an appropriate fee for the implementation of instructions.

It should be specified that the importing processor or subprocessor need only comply with the lawful instructions of the exporting controller/processor (assessed by reference to EU law).

3.2.3. Accuracy (1.4. | page 7)

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 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.

3.2.4. Storage limitation and erasure or return of data (1.5. | page 7)

The data importer's obligations under this clause should apply "after the end of the provision of services relating to processing", as applicable to processors under Article 28. Given the potential complexity of the data importer's systems, it is not realistic to expect or require instantaneous deletion "upon" termination, and it is unclear why the existence of a data transfer should require this when Article 28 does not.

3.2.5. Security of processing (1.6(a) | page 7)

It should be clarified what is 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.

3.2.6. Security of processing (1.6(c) | page 8)

The specific requirements for the data breach notification go substantially beyond what is required of EU processors under 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.

3.2.7. Security of processing (1.6(d) | page 8)

The cooperation and assistance obligations should be better aligned with the obligations to cooperate and assist as set by Art. 28 (3) (f) (g) GDPR.

3.2.8. Documentation and compliance (1.9 | page 9)

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.

3.3. Module Three: Transfer processor to processor

3.3.1. Unclear link to the 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.

3.3.2. Instructions (1.1. | page 9)

The listing of the controllers by the importer/processor poses major problems in our view:

- The list of controllers often corresponds to the processor's customer list. In a significant number of cases, the list of customers will even represent the complete list of the processor's customers. A company will only give such a list to an external party in very limited exceptional cases (e.g. operator of a CRM solution), but not to every subcontractor that might be needed for short term support assignments for customers. The criticality of such a list, which would also have to be dynamically adapted, will usually be quite different from that of personal data, which may only be passed on a need-to-know basis. The necessity of introducing a requirement to compile such a list is also not clear and would in our view need further explanations.

- The list of customers is dynamic and will therefore have to be adapted continuously, as customers will be added continuously while the contractual relationship with others is terminated. In general it should be possible to keep information/annexes online after the new SCC.

- The possibility of the controller being able to issue instructions to the importer directly is problematic. The assumption of costs has not been clarified in this respect and the two parties will not have any direct contractual relations with each other in other respects either. The instruction rights should follow the contractual chain (instruction chain).

- It is also not considered that the importer himself will often not be able to assign data records to a specific controller. In our view, importers/order processors differentiate between the data records of their exporters/customers, but not be-

tween the individual data sets of the end customers (i.e. the actual controller) of their exporters/customers. The direct right of the controller to give instructions will therefore lead to some ambiguity and conflicts with regard to the different contractual relationships of the parties involved, and the risk of data protection violations will increase if importers process the "wrong" data on the instructions of the respective controller.

For the same reasons outlined above, any references to the sub-processing importer making a direct notification to the controller (e.g. Section II, Clause 1.4), responding from enquiries directly from the controller (Section II, Clause 1.9(a)) or having to facilitate the direct exercise of rights (e.g. audit rights) by the controller should be removed. All such rights and obligations should flow via the data exporter.

3.3.3. Security of processing (1.6.(a) | page 10)

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 subprocessor 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.

3.3.4. Security of processing (1.6.(c) | page 11)

This obligation should be amended to be consistent with Article 28(3)(f) GDPR, and so should "tak[e] into account the nature of processing and the information available to the processor".

3.3.5. Documentation and Compliance (1.9 | page 12)

If controllers are given direct audit rights, this leads to a multiplication of audit rights. According to the new SCC not only the exporter can audit, but also all his customers, if necessary. Instead of one audit per exporter, the importer now faces the possibility of hundreds or thousands or even more audits by the controllers.

3.4. Clause 2 Local Laws affecting compliance with the Clause (page 13)(regarding all 4 modules)

The fact that both parties should also issue a warranty that the legal situation in the third country is compatible with the SCC and that a corresponding assessment has been made jointly may be nice from the point of view of the authorities and for the data subjects, since in this respect the exporter and the importer are jointly and severally liable.

For the contracting parties, however, all clauses in the new SCC, where both parties have an equal duty, are not an improvement to the current system. For example, the exporter cannot hold the importer liable for the fact that the importer has given a wrong warranty. The exporter could only hold the importer liable if the importer has not supplied all the information. In this respect, this means that it must be negotiated outside of the SCC who actually takes over certain tasks (e.g. who does the documentation of the evaluation and how the evaluation is carried out). Since it concerns a warranty that both parties have to give up, both parties will want to have a say in the matter, so that a considerable need for coordination (time and financial expenditure) cannot be avoided.

3.5. Clause 3 – Obligations of the data importer in case of government access requests - Notification (page 14) (regarding all four modules)

An obligation of the importer to inform the data subject (possibly with assistance) of the exporter seems counterproductive. In the case of pseudonymized data, the data subject might just get into trouble, because only by re-identifying the data subject the authority could gain knowledge of who the data subject is. The regulation should be limited to the fact that the authority would like to have specific data of a certain data subject, or at least wants to take specific action against the data subject on the basis of data already received.

3.6. Clause 4 – Use of subprocessors (page 16)

Use of Sub-Processors: Module Two/Three Transfer Controller to Processor/Processor to Processor:

The consequences of an objection by the exporter are not regulated. An objection can result in the main contract no longer being able to be executed or only at considerable additional cost. Information in writing about new subcontractors is no longer up to date. Other means of communication (online portal) must remain possible.

If both parties have to keep Annex III up to date, this means that negotiations will again be necessary as to who will actually take over tasks, which in turn increases the time re-

quired. It must also be possible to provide Annex III in an up-to-date manner, e.g. online portal.

Regarding the module for processor to processor: Here, too, it seems impractical for the controller to request contract documents directly from the importer/sub-processor.

Also, an obligation to report any failure seems too far-reaching, which is tantamount to a self-incrimination obligation that would be below the threshold of the reporting obligations of the GDPR.

Clause 4 (e) would mean that the subcontractor must continue to fulfil the contract with the importer vis-à-vis the exporter even though the importer is insolvent, i.e. may no longer pay. A surrender/deletion of the data would still be comprehensible, but it is not likely that subcontractors would agree to a regulation such as provided here.

3.7. Clause 6 (Redress, page 19)

It remains unclear whether this means that the data subject can participate in a "class action" and additionally pursue an individual lawsuit.

3.8. Clause 7 (Liability, page 20)

It is not quite clear whether the liability regulation should be final, i.e. liability regulations which the parties have concluded e.g. in the main contract should have no significance with regard to SCC. For more legal certainty and better risk assessment we suggest amending this paragraph.

4. Section III – Final Provisions

4.1. Clause 1 Non Compliance with the Clauses and termination (page 22):

The clause remains unclear two interpretations of the consequences seem likely:

1. any breach or non-compliance with requirements will result in the consequences set out in the provision: obligation to notify, suspension of the transfer, termination and notification to the authorities

2. the non-compliance with the contract in its entirety will result in the above mentioned consequences.

The effects of the Schrems II judgement show that it is simply not possible to suspend data transfers with immediate effect (without risking irreparable damage). Therefore, a differentiated (risk) assessment would be advisable here as well. If the risks are concrete or abstract, there is a (high) risk of repetition, what data is involved, what consequences threaten the data subject, to name just a few.

Also, it should be clarified that Annex I and Annex III must also be able to be managed in other ways than the suggested options (e.g. online portal).