ACCIS response to the EC consultation on standard contractual clauses (SCCs) for transferring personal data to non-EU countries (Implementing Decision)

10 December 2020

Established in Dublin in 1990, the Association of Consumer Credit Information Suppliers (ACCIS) represents the largest group of credit reference agencies in the world. ACCIS brings together 42 members across 28 European countries and 10 associate and affiliate members from all other continents.

For further details, please visit www.accis.eu

a) Comments on the Implementing Decision

1. Recital (9) and Article 1(1) indicate that the SCCs may be used for transfers of personal data to third parties which are outside the territorial scope of the GDPR. We assume from this that the Commission takes the view that transfers to third parties which are outside the EEA but which are not outside the territorial scope of the GDPR are not restricted by Article 45 GDPR and therefore do not require appropriate safeguards such as SCCs. This is consistent with guidance published by some Data Protection Authorities[1] but it would be helpful for the SCCs to make this point clear as it is not obvious from the GDPR itself.

2. Recital (16) indicates that Module 4 of the SCCs is only for use where a processor within the EU is transferring data to its controller – i.e. the controller on whose behalf it is processing. If that is intended: (a) it would be sensible to make the point more clearly, and (b) there does not seem to be any mechanism in the SCCs for a transfer from a processor to a different controller, on whose behalf the processor is not acting. It is not clear what the parties are supposed to do in those circumstances – for example, is the controller on whose behalf the processor is acting supposed to enter into Module 1 SCCs directly with the importing controller, thereby bypassing the processor? If so, can the processor rely on those controller-controller SCCs when it is not a party to them?

3. Similarly, there does not appear to be a mechanism for a controller within the EU to transfer personal data to a processor which has been appointed by a different controller. Again, it is not clear whether the two controllers are supposed to enter into SCCs directly between themselves, thereby bypassing the processor which is actually receiving the data.

4. Many of the obligations in Module 4 only apply where the processor combines the personal data it has received from the controller, with personal data that has been "collected" by the processor in the EU. It is not clear whether this "collection" would include new personal data which has been generated by the processor, for example as a result of profiling.

5. Recital (20) suggests that, alongside the laws of the destination country, the parties should take into account a range of factors such as the nature of the data transferred, the type of recipient, and the likelihood of public authorities seeking access to the data. This seems inconsistent with

[1] For example, the UK's ICO (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/).

ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

the approach suggested by the EDPB in its recent draft guidance[2], which focuses primarily on the laws in the destination country and suggests that other factors may be "subjective" and should not be taken into account (except to the extent they need to be considered in order to assess whether the relevant laws in the destination country apply to the data transferred). We disagree with the EDPB's position on this and hope to see it follow the Commission's approach in the final version of its guidance.

6. Recital (24) and Article 6 suggest that SCCs based on Decisions 2001/497/EC and 2010/87/EU will continue to be valid for a period of up to one year. Presumably this should also include SCCs based on Decision 2004/915/EC.

b) Comments on the SCCs

Section II

7. Clause 4 of Section I says that the SCCs prevail over any other agreement made between the parties. This should be limited to other agreements which relate to the transfers of data that are the subject matter of the SCCs. Agreements which are unconnected with the transfers described in the SCCs should not be affected.

8. Clause 6 of Section I provides a mechanism for new parties to accede to an existing set of SCCs. Clause 6(c) says that the acceding party will have no rights or obligations arising from the period prior to the date they accede. However, we do not see why the parties should be prevented from agreeing otherwise, and attribute responsibility / liability to the acceding party for the pre-accession period, where this would cater for or enhance the rights of data subjects.

9. The transparency obligations in clause 1.2 of Module 1 in Section II may be difficult to comply with in practice for some types of transfer. There is a disproportionate effort exception in clause 1.2(b) but this will be construed narrowly. Additionally, unlike the transparency obligations in the GDPR itself, no allowance is made for circumstances in which transparency is inappropriate for any of the reasons described in GDPR Article 23. For example, on the basis of Article 23, the UK's Data Protection Act 2018 makes clear that transparency does not need to be provided where personal data is processed for the prevention or detection of crime, and transparency would be likely to prejudice those purposes. It would be sensible for the transparency obligations in the SCCs to include an exception for derogations from the transparency principle which would be available to the parties as a result of EU or national law which complies with the requirements of Article 23. Wording similar to clause 5(f) of Module 1 could be used here.

10. Those transparency obligations also say that the data importer can inform data subjects of the required information either directly or "through the data exporter". However, in many cases it may be appropriate for the information to be provided through a third party, such as the data exporter's clients, where the third party has the relationship with the data subjects and the data exporter and data importer do not. We suggest that that clause 1.2(a) in Module 1 should be amended to read "*… the data importer shall inform them, either directly or through the data exporter or a third party: …*".

11. The obligation to notify data subjects of requests by public authorities should be subject to similar exceptions. For example, clause 3.1(a)(i) requires the data importer to notify data subjects if it receives a legally binding request for disclosure of personal data; in our view, this obligation should only be triggered if the information will actually be disclosed. If, for example, the data importer is able to successfully appeal the request, or if the data is in a form that the data importer cannot access and so cannot disclose (e.g. as a result of encryption) then there is no benefit in informing data subjects of the request.

[2] EDPB's draft recommendations 01/2020.

ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63

12. Clause 1.3(b) of Module 1, clause 1.4 of Module 2 and clause 1.4 of Module 3 (each in Section II) contain an obligation for the parties to notify each other if they learn that the data that has been transferred is inaccurate or outdated. This will often be inappropriate – for example, if the data was only being held for a short period, or was transferred for a single one-off use, it will not be appropriate for the data exporter to notify the data importer of changes to the data after the data exporter should have deleted the original data. Additionally, as in GDPR Article 19, there should be a disproportionate effort exception. As with the transparency obligations, there should also be room for derogations which are permitted by EU or national law in accordance with Article 23.

13. Clause 2(f) of Section II and clause 1(c) of Section III contain termination rights which permit the data exporter to terminate the contract in particular circumstances. The contract in which the SCCs are incorporated may cover a wide range of activities which are unrelated to the international transfer governed by the SCCs, and a data exporter may seek to rely on this termination clause to terminate the entirety of the contract and not merely the part of it that relates to the transfer of data. We suggest that the termination provision should be changed into a right to suspend the transfer.

14. Given that the SCCs prevail over any other terms agreed between the parties (see clause 4 of Section I), the liability terms at clause 7 and the indemnity at clause 8 may upset the apportionment of risk that the parties have agreed in the wider commercial arrangement in which the SCCs are incorporated. Although we would accept that the parties should not be able to unreasonably restrict their liability to data subjects under the SCCs, we do not see why the SCCs should interfere with the liability arrangements that have been agreed between the parties to the SCCs. Additionally, it is questionable whether clause 7(b) will be valid under the relevant governing law[3]. It is unclear how clause 7 would interact with other liability terms agreed between the parties which *do* comply with the requirements of national law.

Section III

15. Clause 1(d) suggests that, for Module 4 (i.e. where a processor is transferring data to the controller for which it is processing data), the controller must destroy the transferred data if the contract is terminated. However, this is likely to consist of data which originated with the controller and was merely being processed on its behalf in the EEA by the processor. We do not see why the controller should be required to delete the data that it has received back from the processor in those circumstances.

16. Clause 2 requires the parties to choose the law of an EU Member State to govern the contract. We do not see why the governing law must be the law of a Member State, provided that the law chosen allows for third party beneficiary rights and otherwise provides adequate recourse for the parties and for data subjects[4].

17. Similarly, clause 3 requires the parties to choose the courts of an EU Member State to resolve disputes. There is no obvious reason why the parties are only able to choose the courts of an EU Member State to hear their disputes. In the case of disputes between the parties, those courts may not be convenient (particularly where the SCCs are used for onward transfers which may not involve any party located within the EU), and in the case of disputes with a data subject, the data subject themselves might not reside in the relevant Member State (or any Member State at all) and so the courts chosen may not be convenient for them either.

We thank you for your attention and remain available to discuss these issues further.

[3] In England and Wales, for example, it is not possible to exclude or limit liability for death or personal injury caused by negligence, and so it is common to stipulate that liability exclusions do not apply to those kinds of liability. If that is not done then the entire clause risks being found to be invalid.
[4] For example, the law of jurisdictions within the UK ought to be acceptable.

ACCIS IVZW • p/a Interel • Rue du Luxembourg 22-24 • B-1000 Brussels
+ 32 2 761 66 93 / secretariat@accis.eu / www.accis.eu / EU Transparency Register: 21868711871-63