EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

10 December 2020

EACA Comments on the Draft Implementing Decision and Annex on standard contractual clauses for the transfer of personal data to third countries

EACA welcomes the opportunity to provide feedback on the Draft Implementing Decision (Ref: Ares(2020)6654686) and Annex (Ref: Ares(2020)665468) on standard contractual clauses for the transfer of personal data to third countries pursuant to the General Data Protection Regulation (GDPR).

EACA represents more than 2,500 communications agencies and agency associations from nearly 30 European countries that directly employ more than 120,000 people. EACA members include advertising, media, digital, branding and PR agencies.

We would like to share the following concerns and suggestions for improvement on behalf of our membership.

1. Repealing existing SCCs will result in unnecessary administrative burden (Draft Implementing Decision, Art. 6,3)

We believe that there is no need to limit the continued reliance on *existing* SCC to one year.

Suggestions:

- We feel that existing SCCs should remain in force for an indefinite period, or at least for a period of three years.
- The new/updated SCC should be used for *new* cases only. While SCC that are currently in place may require modernization, they do fulfill the requirements of the GDPR.
- Following a risk-based approach, new SCCs should only be mandated where high risk data (e.g. sensitive data) is involved,
- In addition, they should be updated by means of a standard addendum, drafted by the Commission, that could be added to Article 6, above.

2. Requiring a direct controller – sub-processor relationship could have unintended consequences (Section I, Clause 1(b)(ii), Section II Module 3 Clause 1.6 (c), Section II Module 1.9 (c), Section II Clause 4(a))

Whereas data controllers, due to the need to approve the use of sub-processors, may know the sub-processor, the sub-processor may not necessarily know the controller.

Requiring a direct relationship between controller and sub-processor defeats the purpose of having a processor – (sub)processor SCC.

Avenue Louise 120
1050 Brussels, Belgium
+32 2 740 07 10
+32 2 740 07 17
info@eaca.eu
www.eaca.eu

Controllers, contrary to processors, usually do not have close working relationships with sub-processors. Mandating direct communications and audits between the controller and sub-processor can have the following adverse effects:

- Controllers could become more inclined to work directly with sub-processors and to cut out (European) processors, putting the latter in existential problems.
- Sub-processors might be reluctant to have their business secrets (e.g. pseudonymization techniques, data de-duplication techniques used for better protection and data accuracy) exposed to yet another company, potentially causing European companies to lose the possibility to use such (sub-)processors.
- In addition, (EU) controllers might be exposed to more direct liability to be accountable for the sub-processor's level of compliance.

In the case of advertising, the controllers are usually advertisers, who will inevitably want to transfer liability to the processor. Sub-processors, on the other hand – especially those with a market-dominant position – often operate on fixed terms. Processors might therefore not be in a position to require their sub-processors to meet the controllers' obligations. Under the current draft SCC, therefore, processors might be "caught in the middle – liable to the controller for sub-processors, while sub-processors might refuse to accept the controllers' terms. Processors could end up being liable for the whole data transfer chain.

Suggestions

- Controllers should not have the right to audit sub-processors
- The requirement that sub-processors inform further appointments of sub-processors should be removed (Section II Clause 4(a))
- The processor, not the sub-processor, should inform the controller of relevant breaches (Section II, Module 3, Clause 1.9 (c)).

3. The burden, specifically on SMEs, needs to be alleviated (e.g. Section II Clause 2(d), Section II Clause 3 3.1 (b))

Not all companies have legal departments and/or legal subscription services that monitor relevant legal changes on their behalf. This is the case for the majority of small communications agencies. In addition, liability increases disproportionately for them when they bear the responsibility of ensuring legal changes on top of other requirements set out in the SCC.

Suggestions

- Monitoring for changes in the level of risk to data protection of all countries and sectors should be done centrally and published by the European Commission.
- Measures to be implemented should be determined on a case-by-case and risk basis to ensure that the effort and protection provided is proportionate and appropriate.

Avenue Louise 120
1050 Brussels, Belgium
+32 2 740 07 10
+32 2 740 07 17
info@eaca.eu
www.eaca.eu

The following clauses, which risk putting unquantified open-ended financial burden on the data importers, should therefore be changed (see strike-throughs)

- *Section II Clause 3 3.1 (b) If the data importer is prohibited from notifying the data exporter and/or the data subject, the data importer agree to ~~use its best efforts to obtain a waiver of prohibition with a view to~~ communicate as much information and as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them upon request to the data exporter.*

- *Section II Clause 3 3.2 Review of legality and data minimization a) the data importer agrees to review, under the laws of the country of destination, the legality of the request for disclose, notably whether it remains within the powers granted to the requesting public authority and to ~~exhaust all available remedies to challenge the request~~ if, after careful assessment, it concludes that there are grounds under the laws of the country of destination to do so. When challenging a request, the data importer shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules […]*

4. Some obligations and requirements appear to be disproportionate, ineffective and burdensome

These include, for example:

- Obligations to do a transfer-risk-assessment in all cases (Section II, Clause 2 (d))
- Requirements to list all controllers in a processor-to-processor scenario (Section II, Clause 2 (d))
- Requirements to notify competent authorities (Section II, Module 1, Clauses 1.5 (d) and (e)

In addition, Clause 2 (a), especially when it comes to **data access by authorities in third countries**, seems very vague and therefore difficult to fully comply with in all circumstances. We believe that the applicability and compliance with requirements set by third countries' authorities should not be left entirely to the parties involved. Data importers have too many obligations, many of which result in a discretional analysis (e.g. with regards to the provision of warranties until 2 a)) and could lead to deficient evaluation. This could be complicated by the fact that other authorities may come to different evaluations than the parties involved and/or an additional authority enters the evaluation. Given their margin of discretion, this could lead to quite different and inconsistent evaluations.

Also, with regards to the **EU processor – third country-controller transfer scenario** (Clause 2, module 4), including the reference '*only if the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU*", might be of limited use, since it is unlikely that the controller does not have to appoint a representative as per the GDPR.

For more information or questions, contact:

Nina Elzer
Senior Public Affairs Manager
EACA – European Association for Communications Agencies
Tel: +32 (0)2 740 07 13
nina.elzer@eaca.eu