CONSULTATION OF THE EUROPEAN COMMISSION ON STANDARD CONTRACTUAL CLAUSES ("SCC")

AFEP's comments

The European Commission's DG Justice hold until December 10 a consultation on its draft implementing decision on standard contractual clauses ("SCC") for the transfer of personal data to non-EU countries.

The update of these SCC by the European Commission follows a consultation earlier this year and aims to include both new requirements from the GPDR and consequences of the recent judgment C-311/18 of the CJEU ("Schrems II" case). This judgment essentially invalidates the Privacy Schield (the adequacy decision with the United States) and confirms the validity – under certain conditions – of the standard contractual clauses which allow transfers to countries for which adequacy agreement do not exist (hereafter "third country").

The draft decision - and the conditions posed by the CJEU incorporated in it - calls for the following comments from companies:

- *Positive aspects :*

AFEP member companies positively note that the European Commission is working on the SCC remaining GDPR compliant on various points. In particular, they appreciate:

- the modular approach proposed by the Commission to cover the complexity of scenarios and contractual relationships (in particular the relationships between subcontractors and tier-2 subcontractors),
- the risk-based approach to be carried out by the data exporter and the data importer[1] that ensure full consistency with the overall GDPR requirements,
- the role given to the data importer who must, in particular, comply with its contractual commitments under the SCC and ensure that the personal data are adequate, relevant and limited to what is necessary to the purpose(s) of processing[2],
- the explicit exclusion of any punitive damage[3].

- *Negative aspects :*

They express, however, serious concerns on two major points which condition the effective implementation of these clauses.

i) The analysis of local laws and possible additional measures: a disproportionate and non-GDPR-compliant burden for private actors

Economic actors exporting data to third countries ("data exporters") must assess whether the legal framework and practices of these third countries undermine the effective protection of data transfer tools[4].

[1] Annex to the Commission implementing decision on SCC for the transfert of personal data to third countries – Section II – Obligations of the parties, § 1.5 Security of processing -a)
[2] Section II – Obligations of the parties - § 1.3- c)
[3] Section II- clause 7 –Liability- b)
[4] Section II – clause 2 - Local laws affecting compliance with the Clauses

- The European Commission demands that these actors guarantee ("warrant") the adequacy of the third country legal framework with European rules in view of the specific circumstances of the transfer; within this legal framework, the data access required by certain authorities or governments of third countries is expressly mentioned;
- If inadequacies are found, the Commission requires the data exporter to take additional measures to address these local impairments to the effective implementation of the European framework (clause 2-f);
- If the adoption of such measures is not possible, then data transfer should be avoided, suspended, or stopped.

This analysis by the data exporter, with the collaboration of the data importer making his "best efforts" (clause 2-c) would be required for both to the general legal framework and the specific circumstances of each transfer (clause 2-b).

AFEP opposes this procedure as it calls into question the provisions of the GDPR:

- *regarding efficiency*: private economic actors ("data exporters") wishing to transfer - or having for many years - their data in third countries will now have to analyse the adequacy of the national laws concerned.

    - Within the framework of the GDPR, it is the responsibility of the European Commission to assess the suitability of third countries (article 45). Until now this "white list" was adopted by the Commission and created a common and stable legal framework. The draft SCC propose that companies replace the Commission, develop their own "private blacklists" of countries that do not comply with the GDPR, and later update them if this legal framework changes. Adequacy assessments should therefore be conducted by the Commission or the EDPB. They should maintain a database of adequacy assessments at the EU level, which could evolve as laws and practices change, and be freely available to organisations.
    - It is essential to maintain the hierarchy provided for by the GDPR in the mechanisms allowing the transfer. For the same country, divergent interpretations will not allow proper application of SCC and, more generally, of data protection measures; such a divergence of views is contrary to the objectives of consistency sought by this tool and a source of great legal uncertainty for economic players,
    - Without this general consistency, the usefulness of the SCC is questioned, since additional due diligence on a case-by-case basis would be required, while they aimed to provide a global legal framework to the actors operating transfers.

- *in terms of responsibility*: according to the project, "data exporters" are primarily responsible for such an analysis and for additional measures to be taken, if necessary. In the absence of an assessment by the Commission or by the Data Protection Authorities as provided for by the GDPR, this task must fall to the data importer. He indeed would have a better knowledge of his own country's regulations, and his assessment would guarantee the quality of this analysis.

ii) the date of entry into force of this decision: to be postponed while avoiding any retroactivity

All of these measures must be implemented within one year from the date of entry into force of the European Commission's decision to replace the existing SCC.

Imposing such complex measures to be implemented in such short time frames will be a challenge for many companies of all sizes. If GDPR compliance is not to be ensured, it is required to suspend data transfer and terminate the contract[5]. But what is the consequence for the data for which the processing would be suspended? How to replace the usual "data importers" and how can we be sure that the implementation deadlines imposed by the Commission are respected?

This very tight calendar constraint also induces for European companies high risks of sanctions (up to 4% of their worldwide turnover) or undesirable reputation in this complex economic period.

AFEP, therefore, recommends the following methods:

- *carry out a real impact study* on the modifications envisaged in this project: as underlined in point (i), these are both costly and disproportionate. In accordance with the provisions of the GDPR, it is up to the Commission to study their adequacy with the existing legal framework and the resulting administrative burdens. For them to do their best, it is essential that European economic actors have easy access to a clear legal framework summarizing this adequacy analysis,
- *postpone the implementation of these provisions from 1 to 3 years*: similar past experiences have shown that a period of one year does not allow for the operational implementation of new requirements (e.g the guidelines of the European Banking Authority on outsourcing arrangements published in February 2019 provide for compliance no later than December 2021 for current contracts. By pragmatic analogy, a period of three years should be favoured),
- *avoid any retroactivity by specifying the scope of this draft*: only new SCC projects should be affected by these new constraints, except for ongoing contracts. As many contracts are valid beyond this single year, their SCC should remain valid until their expiration or renewal. With the current SCC having offered an adequate level of protection and guarantees for several decades and the parties already being required to check whether additional measures need to be put in place, the request to update all contracts seems unhelpful and extremely burdensome. Requiring importers and exporters to apply the revised SCC only to new contracts will suffice to meet the requirements in terms of securing data transfers in third countries.

***

AFEP member companies fully support the ambitions of the European Commission to enforce its personal data protection standards in favour of its European citizens, consumers, or employees. However, this must go hand in hand with smooth flows of data worldwide (see in this sense the management of employee data) and no unnecessary and disproportionate companies' administrative and financial constraints.

The difficulties, encountered for several years by government institutions, in providing a stable and secure legal framework for transfers outside the European Union -after having encouraged exchanges between open economies and the development of information transfers- should not lead to putting all the risks associated with these transfers on data exporters only.

AFEP companies are prepared to work in close collaboration with the supervisory authorities and the main IT service providers to find realistic solutions (mutualisation of part of the analysis, revision of additional measures, valuation of the risk-based approach) to maintain transfer

[5] Section II- clause 2- f)

operations that are a key part of their operation and development and are strategic for European global competitiveness.

***

ABOUT AFEP

Since 1982, AFEP gathers the largest companies present in France. The association, based in Paris and Brussels, aims to foster a favourable environment for businesses and to present the vision of its members to French public authorities, European institutions and international organisations. Restoring business competitiveness to achieve sustainable growth and employment in Europe and meet the challenges of globalisation is AFEP's priority. AFEP has around 113 members. More than 8 million people are employed by AFEP member companies and their cumulative annual turnover amounts to 2,600 billion euros.

CONTACTS

Emmanuelle Flament-Mascaret – Director of Business Affairs and Intellectual Property concurrence@afep.com

Alix Fontaine – EU Public Affairs Advisor - a.fontaine@afep.com