# CONSULTATION OF THE EUROPEAN DATA PROTECTION BOARD (EDPB) ON ITS RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOL TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

## AFEP (French Association of Large Companies)'s comments

The European Data Protection Board (EDPB) hold until December 21 a consultation on its Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

This Recommendation appears as a necessary upgrade following the recent judgment C-311/18 of the CJEU ("Schrems II" case). This judgment essentially invalidates the Privacy Shield (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").

- While companies appreciate the EDPB' effort to provide a clear procedural framework allowing coherent application by supervisory authorities and European economic players, they nevertheless express serious concerns. Two points stemming from the conditions imposed by the judgment the CJEU are particularly complicating the effective implementation of these clauses.
- In this context, AFEP member companies recommend the suspension of the application of this Recommendation and the start of in-depth discussions between the authorities and the European economic actors to resolve these issues as well as possible.

### 1. Serious concerns on two major points:

#### *i) The analysis of local laws and possible supplementary security measures: an inadequate 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.

- The Recommendation requires (step 3) that data exporters guarantee ("you must assess") the adequacy of the general legal framework of the third country to European rules in the context of the specific transfer; in this legal framework, access to data required by certain authorities or governments of third countries is expressly mentioned;
- If inadequacies are found, the EDPB requests (step 4) from the data exporter to take supplementary measures to address these local inadequacies with the level of protection equivalent to that guaranteed within the EU; among these measures is the encryption or pseudonymisation of data (§ 49);
- If the adoption of such measures is not possible, then the data transfer should be avoided, suspended or stopped.

AFEP cannot accept this assessment roadmap. It calls into question the provisions of the GDPR, which instructs the European Commission or the supervisory authority to adopt standard data protection clauses (article 46-c and d). This "white list" adopted by the Commission creates a common and stable legal framework. The EDPB recommendation reverses this logic by proposing

that companies replace the Commission, develop their own "private blacklists" of non-GDPR-compliant countries and later update them if this legal framework changes.

Furthermore, this approach is legally irrelevant and technologically unrealistic:

- Legally, it is not reasonable to consider that contractual clauses and supplementary measures may have a greater legal value than local laws,
- Technologically, no European operator can at this stage propose to European companies a comparable technological and efficient offer as the one deployed by American players (maintenance, flow speed, etc.). In addition, existing European players such as the German operator SAP cannot prevent remote access from third countries, which crystalises some of the concerns of the European judge.

The EDPB increases the burden on European data exporters:

- *In terms of efficiency:* private data exporters wishing to transfer - or have for many years - their data in third countries will now have to analyse the adequacy of the national laws concerned. This is a heavy burden for one company. Clearly, it would be much more efficient if the bulk of the assessment were carried out collectively by the authorities regulating European companies.

    - It is essential to maintain the hierarchy provided for by the GDPR in the mechanisms allowing the transfer. For the same country, divergent assessments made by different companies will not allow proper application of SCC and, in general, 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.
    - Adequacy assessments should therefore be carried out by the Commission or the EDPB who should maintain a database of assessments at European level, which may evolve as laws and practices change, and which would be freely accessible to organizations.
    - Without this general consistency, the usefulness of 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 for actors operating transfers.
    - Supplementary measures - such as data encryption - increase the burden on companies whose international development will be considerably hampered. The encryption of any type of data located or accessible from a non-GDPR compliant third country would complexify exchanges between a company and its subsidiaries, for example to finalise a commercial contract or manage careers.

- *In terms of process*: the entire procedure is cumbersome, expensive, and long; this multiplication of administrative burdens does not seem to comply with the spirit of the GDPR, which advocates for a risk-based approach: here, the same constraints are required regardless of the type of data transferred (sensitive or not, biometric, financial and "critical", B2B, B2C, etc.) whereas:

    - Some countries such as Australia or India make this distinction, which de facto lightens the burden on economic players;
    - The American laws governing government access to data ("FISA 702" in particular) also differentiate the data: for example, HR data is not affected;
    - The risk of being subjected to a data request varies according to the business model of the exporter and the importer (data transfers for commercial purposes or social networks), and according to the category of data (commercial data or personal data).

- *In terms of responsibility:* according to the Recommendation, "data exporters" are primarily responsible for such an analysis and for supplementary measures to be taken, if necessary. For the reasons mentioned above, this should not be the case. This assessment must primarily be the responsibility of the European Commission or the Data Protection Authorities, in accordance with the provisions of the GDPR. Otherwise, this task should 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*

All the measures of this Recommendation are immediately applicable.

Implementing such measures is an unrealistic challenge for businesses of all sizes. If GDPR compliance is not assured, it is required to suspend data transfer and terminate the contract. The question of the consequence for the data for which the processing would be suspended and of the replacement of the usual "data importers" must be absolutely raised before forbidding any action.

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

AFEP therefore recommends the following methods:

### *(i) Develop adequacy decisions*

Companies would like to rely more on adequacy decisions than on standard data protection clauses or binding corporate rules. It is therefore important to increase the number of adequacy decisions, and to establish priorities in doing so, without giving up on an imperative equivalent level of protection.

First, companies emphasise the value of quickly adopting adequacy decisions for third countries with which the volumes of material and digital exchanges are significant (Australia, Brazil, Great Britain, India). They welcome the approach taken with Japan which has consisted of pairing the negotiations of the Economic Partnership Agreement with the process of adopting twin adequacy decisions.

On a secondary basis, a solution could be to speed up and/or simplify the adoption of an adequacy decision with countries which not only have an equivalent level of protection but also fairly similar legal architectures, with in particular a decisive role granted to independent data protection authorities.

At the very least, it is essential that the European authorities assess the adequacy of the national systems of third countries and specify the difficulties they present regarding the GDPR.

### *(ii) Ultimately, adopt a more flexible approach to data transfer in case of legal convergence*

With an increasing number of countries adopting data protection regimes inspired by the GDPR, it would be desirable for the EU to opt for a new approach to the transfer of data to third countries, with as a basic principle, the free transfer of personal data to third countries when their legal system guarantees an equivalent level of data protection (subject to public policy exception). This new approach does not necessarily mean questioning the adequacy decisions but could result in them

being easier to adopt and in the EU adopting a logic of blacklists of countries to which transfers would be prohibited and/or restricted.

This approach would also facilitate the conclusion of data provisions in free trade agreements since most third countries accept the standard adopted in the Trans-Pacific Partnership Agreement which recognises the principle of free transfer of non-personal and personal data, with limits related to public policy objectives of personal data protection.

*(iii) Suspend the implementation of these provisions*

The immediate application of this Recommendation is unrealistic for economic agents. 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 three-year grace period should be preferred.

This period would allow to:

- consider the differentiation of the type of data (sensitive or not, BtoB / BtoC) covered by this recommendation in accordance with the risk-based approach advocated by the GDPR; it should be noted that the European Commission's SCC project has a proportionate approach in this area;
- to do so, establish a list of data not subject to Section 702 of the "Foreign Intelligence Surveillance Act" ("FISA 702"); such a list would alleviate the constraints for companies and bring more solid legal bases to a future adequacy decision;
- review some examples produced in appendix 2 of the Recommendation: use cases 6 and 7 illustrating examples of inappropriate supplementary measures are too broad in their application and lead to blocking situations for companies with subsidiaries in many countries.

*(iv) 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 supplementary 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.

But at this stage, this Recommendation is leading European companies into a legal and technological deadlock. It charges them with a responsibility going beyond the provisions of the GDPR without providing them with any pragmatic solutions.

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 just data exporters.

AFEP companies propose 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 supplementary measures, valuation of the risk-based approach) to maintain transfer operations that are a key part of their operation and development as they 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