Public consultation on the roadmap by the European Commission on the GDPR application report

ANSWER FROM AFEP (FRENCH ASSOCIATION OF LARGE COMPANIES)

The European Commission launched until April 29 a public consultation on its **roadmap** for the **report on the application of the general data protection regulation** (GDPR), which will be made public by 25 May 2020. This report intends to identify potential problems in the application of the GDPR, in particular as regards the issue of **international transfer of personal data to third countries and existing adequacy decisions** (Chapter V) as well as the **cooperation and consistency mechanism between national data protection authorities** (Chapter VII).

French companies substantially ask for:

- an **evolution of the approach on data transfer towards more liberalisation**, given the growing convergence of personal data protection regimes;
- being able, in any case, to **rely more on adequacy decisions** rather than using by default alternative instruments (binding corporate rules and above all standard data protection clauses) and therefore for an **increase in the number of adequacy decisions** and the **acceleration of their adoption procedures;**
- to do this, a **clarification of the criteria** on which the European Commission takes adequacy decisions, with a priority notably given to the countries with which free trade agreements are negotiated and the countries with the closest legal architecture;
- **strengthening reciprocity in data exchanges** by using free trade agreements as leverage, and including it as an **explicit and mandatory criterion for the adoption of adequacy decisions**;
- **better coordination of national authorities** for the implementation of this regulation;
- **greater harmonisation of practices and interpretations;**
- an **update of certain provisions**.

1. ON CHAPTER V

Large companies carry out numerous transfers of personal data to third countries based on Chapter V of the GDPR, of which they appreciate the principle of extra-territoriality. However, the reality of these exchanges outside the EU leads them to underline the need for the European Commission to correct various shortcomings or inaccuracies during the preparation of its future report. Some of these corrections are related to **adequacy decisions (art 45) and standard contractual clauses ("SCC" - art 46),** which are major tools in companies daily-life for both the practical circulation of these data flows and the related legal responsibility ("accountability").

- **Current limits in the use of data transfer tools to third countries**

Companies have learned to use solutions such as adequacy decisions like the “Privacy Shield” or the instruments provided for in articles 46 and 47 of the GDPR (in particular the company rules binding or standard data protection clauses) as data transfer tools to third countries.

However, they believe that, given the increase in transfer volumes linked to the development of digital technology and industrial applications (Internet of Things), they should be able to have access to more global, more efficient and better-articulated solutions.

- **Revision of the overall architecture of the mechanism for the transfer of personal data in the light of the convergence of legal data protection systems**

The EU approach to data protection has been widely documented and an increasing number of third countries are setting up personal data protection regimes whose principles are converging with those of the EU, including within the United States (cf. legislation adopted by the State of California).

This dynamic should lead to a new approach to the transfer of data to third countries, with the basic principle being 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 principle of adequacy decisions but could lead to their easier adoption and to the EU adopting blacklists of countries to which the 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 Transatlantic Partnership Agreement, which recognizes the principle of free transfer of non-personal and personal data, subject to limits related to public-policy objectives in data protection.

- More numerous and prioritized adequacy decisions

In any case, companies would rather rely on adequacy decisions than on binding corporate rules or standard data protection clauses, even if they recognize that the adequacy regime must sometimes be combined with them (especially in the case of the Privacy Shield).

It is therefore important to increase the number of adequacy decisions and, to do so, to establish priorities without renouncing the imperative of an equivalent level of protection.

Firstly, companies stress the importance of adopting adequacy decisions quickly for third countries with which the volumes of material and digital trade are significant (Australia, Brazil, Great Britain, India). They welcome the approach followed with Japan, which has been to combine the negotiations of the Economic Partnership Agreement with the process of adopting twin adequacy decisions.

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

An adequacy decision with the United Kingdom must therefore be the main priority: it is both a leading economic partner and a country whose legal data protection system, even after its withdrawal from the EU, is modelled on that of the GDPR.

- Better consideration of the reciprocity of transfers of personal data

Companies are committed to ensuring the level of protection provided by the GDPR in their transfers to third countries but also wish to be able to transfer personal data from third countries. However, this reciprocal liberalisation continues to come up against some protectionism of personal and non-personal data.

The process to obtain twin adequacy decisions with Japan is an important step towards this goal of reciprocity.

Two elements could further strengthen the reciprocity requirement:

(1) On the one hand, the approximation of the EU position with those of its main trading partners on trade agreements' provisions on personal data, which would make it possible to demand in return the same degree of openness in data transfers to the EU;
(2) In any case, to include reciprocity as an explicit and mandatory criterion for adopting an adequacy decision. This clarification would constitute a leverage effect on our partners.

- Need to make adequacy decisions even more efficient

As data transfers to third countries require adequate levels of protection defined by the European Commission, companies deplore the fact that tools as essential as the "Privacy Shield" are not fully deployed and, therefore, would like additional clarifications aiming both already existing decisions (future revisions) and coming ones:

- the operating methods of the **authorities of third countries**: they have the reputation of enforcing the GDPR and assurances in this regard must be better considered by the European Commission;
- the **obligations to perform an audit** on IT security, in particular, that data processors must facilitate to ensure the protection of personal data in real adequacy with European regulations (article 28);
- the **analysis criteria** used to consider and conclude adequacy decisions with third countries.

- **Updating the provisions relating to standard contractual clauses ("SCC")**

- the reference to the **1995 directive must be deleted and must be accompanied** by the confirmation that the SCCs signed since the entry into force of the GDPR remain valid;
- the conditions **for handling personal data to be fulfilled by the processor** from a third country should be specified (place of transfer and type of data concerned);

2. ON CHAPTER VII

Companies strongly emphasise and deplore the **lack of harmonisation between supervisory authorities** in their approach and implementation of the European regulation, a legal instrument chosen to reinforce the necessary harmonisation for the fluidity of the management of personal data within the single market and in third countries.

The heterogeneous implementation of this text by the national authorities complicates the life of companies (administrative burdens, legal uncertainties, etc.) even though their responsibility has been reinforced. It can also be a source of distortion of competition within the single market since it involves different obligations and burdens for companies based in the European territory and acting on the same market but dependent on different reference authorities.

Varied interpretations are thus deplored in several fields such as:

- sales on the Internet, conditioned by the French authority to the collection of the prior consent of people on their bank data, while these can be collected without express consent by all companies based outside France;
- the management of cookies consent, which are subject to well-known different application recommendations between EU member states;
- the duration of data storage, framed by national standards, which makes the management of this subject complex, risky and time-consuming in the context of international transfers.

Companies therefore wish to see many improvements in this cooperation and this coherence mechanism dealt with in Chapter VII.

These improvements should, in particular, be based on the framework recalled by a recent judgment of the CJEU on the occasion of a reference for a preliminary ruling. The Court stated that the Member States "*cannot add new principles relating to the lawfulness of the processing of personal data in that article or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article*".

The CJEU refuses that a State predetermines the choice of a legal basis or its conditions of application. The GDPR is opposed to a Member State categorically and generally excluding the possibility for certain categories of personal data from being processed, without allowing balancing of the opposing rights and interests involved in a particular case.

This approach, which aims at greater harmonisation within the Member States, is welcome and should help to simplify the procedures for businesses vis-à-vis the Commission and national authorities. The strengthening of this harmonisation must be accompanied by various provisions related both to the European Data Protection Supervisor (EDPS) and to the concept of lead authority.

• Strengthening of the powers of the EDPS

- national recommendations taken on the interpretation of the GDPR should be submitted more systematically to the Committee's opinion, in particular when the recommendation of an authority relates to the legal basis for the processing of data and tends to impose the choice of this basis (in accordance with Article 63 of the GDPR);
- recommendations accompanied by sanctions concerning the interpretation of the GDPR should only be able to be taken by national authorities after the guidelines of the European Committee proposing a harmonised interpretation have been issued. If necessary, a moratorium on the application of the national recommendation and sanctions should be taken by the local authority;
- the EDPS being the guarantor of the consistency of the interpretation of the GDPR, it should be able to be contacted directly by companies or individuals regarding the consistency of certain opinions or recommendations issued by local authorities on the basis of local processing;
- the EDPS should make his work and items on the agenda more transparent (for example, the French CNIL has indicated for over a year that the subject of the storage of banking data is on its agenda and that work is in progress on the elaboration of a joint recommendation, but the agenda of the EDPS does not mention it).

• Details on the competent lead authority:

Presented during the development of the GDPR as an essential tool for ensuring consistency of national approaches, the implementation of the powers of the "lead" authority should be made more efficient by:

- increasing transparency on the relations between the competent lead authority and national authorities (for example, no information is given on a possible referral to the Luxembourg data protection authority for complaints concerning the retention of banking data of Amazon's French customers, or if other national authorities have been seized);
- considering a system which would allow, once a certain number of complaints from nationals have been lodged, that the competent lead authority divests itself of the file in favour of the national authority concerned.

***

About AFEP

Since 1982, AFEP brings together large companies operating in France. The Association, based in Paris and Brussels, aims to foster a business-friendly environment and to present the company members' vision to French public authorities, European institutions and international organisations. Restoring business competitiveness to achieve growth and sustainable employment in Europe and tackle the challenges of globalisation is AFEP's core priority. AFEP has around 113 members. More than 8 million people are employed by AFEP companies and their annual combined turnover amounts to €2,600 billion.

Contact:
Emmanuelle Flament-Mascaret, Director for IP and Commercial Affairs / e.flament-mascaret@afep.com
Marc Poulain, Director for International Trade Negotiations / m.poulain@afep.com