December 2012

PROPOSAL FOR A GENERAL DATA PROTECTION REGULATION

AFEP'S MAIN OBSERVATIONS

AFEP represents more than 100 of the top private sector companies operating in France. AFEP's purpose is to present the views of large French companies to the European Institutions, international organisations and the French authorities, mainly with regard to the drafting of non-sectoral legislation.

French companies, which have long been committed to data protection, support the European Union's initiative to **harmonise Data protection rules** and so **reduce unnecessary administrative burdens**. In particular, AFEP **welcomes the establishment of a 'one-stop shop'** providing the opportunity to simplify companies' dealings with national supervisory authorities.

However, AFEP regrets the Commission's proposed shift, leading the EU to focus on punishing rather than preventing offences. In this context, companies can only support a **system of sanctions that are directly proportional to the severity of breaches** observed.

I- Context

At the end of January 2012, the European Commission (EC) published two legislative proposals on personal data protection, namely a Directive on the processing of such data in criminal matters and a general **Regulation on "the protection of individuals with regard to the processing of personal data and on the free movement of such data" repealing the 1995 Directive**.

Member companies have given serious consideration to the proposed Regulation. The Commission's intention is not only to ensure greater respect for the privacy of citizens, but also to take better account of the data flows at global level and the role played by the Internet.

II- AFEP's position

1- Main positive breakthroughs in the proposed Regulation

Even though improvements still need to be made, it is appropriate to review the current texts, particularly given the development of the Internet. Consequently, **AFEP supports the harmonisation approach** undertaken by the Commission.

a- '***One-stop shop***'

Member companies are in favour of a '**one-stop shop**', the aim of which is to harmonise, simplify and centralise their dealings.

The one-stop shop would come into effect where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in several Member States. In this case, the competent authority of the company's **main establishment** would be competent.

The notion of main establishment (Article 4-13, recitals 27, 97 to 99) is therefore the cornerstone of the one-stop shop. However, it should be organised so as to best correspond to the structure of large companies.

In Article 4-13, controller's main establishment is where the main decisions are taken. Given that the one-stop shop is designed to facilitate matters for companies, the flexibility provided should thus be confirmed. **Consequently, the list qualifying these decisions as to the purposes, conditions or means of processing should be alternative and not cumulative, by replacing "and" with "*or*".**

b- Binding corporate rules (BCRs)

The opportunity to adopt BCRs, already widespread within large companies, entails substantial advantages. In fact, while the existence of BCRs must still be notified to and approved by the national authority, this obligation would now be removed in the case of international transfers of data, so reducing administrative burdens (Art. 43 § 2-b).

In this context, AFEP proposes **that the opportunities of international transfers be extended** beyond a group of undertakings within which BCRs are applied, **to separate undertakings which each have their own BCRs**.

2- AFEP's main concerns

a- Sanctions: to be proportional to the breach observed

In addition to criminal sanctions relating to the controller or a representative, Articles 78 and 79 set out three types of **administrative sanctions**. Their severity depends on the breach observed. They are applicable to large companies and range from **0.5% to 2% of their global annual turnover**.

The proposed percentages **are out of proportion** with the offences committed and the damage caused. **For example**, some large companies in France could be forced to pay a fine potentially in excess of EUR 1 billion because they have omitted to provide a copy of the personal data in electronic format to the data subject (Art. 79-5, d). Penalising straightforward cases of "**negligence**" by such an amount is disproportionate.

By way of comparison, in the sphere of competition law, high fines may be justified in the light of the damage to the economy caused by the anti-competitive practice penalised. In contrast, while data protection is a fundamental right, **the damage in this case cannot be considered to be equivalent to the damage to the economy**. Consequently, the sanctions imposed cannot be equivalent.

Furthermore, not only are the **calculation methods not specified** (is the turnover that of the undertaking or the group of undertakings?), but these amounts are also potentially higher than those in the sphere of employment law.

Consequently, rather than a percentage, member companies call for a sanction upper limit of **up to EUR 1 million, the upper limit mentioned in Article 79-6, and for this sanction to be proportional to the breach observed**.

b- Explicit consent: to be restricted to sensitive data

Covered in Articles 4-8, 6, 7 and 9, the concept of consent is now based on "explicit" consent (opt-in).

Given increasingly rapid exchanges, the requirement of explicit consent for each transaction is problematic in terms of **technical feasibility**. It **would indeed slow down service offering and innovation**. The very aim of revising the 1995 Directive, which is to take into account recent technological developments, does not seem to be achieved in this respect.

We need to **maintain the opt-out** of the 1995 Directive, with **the opt-in being restricted to the processing of the most sensitive data**, as defined in Article 9 of the proposal for a Regulation.

c- The right to be forgotten: to be adapted

Article 17-2 states that **the controller is responsible for informing third parties** when a data subject requires to erase any links to or copy of these data.

It is important to take better account of the reality and the limits of the relationship between the controller and the third parties. While, technically, the controller has the means to manage the data for which it is responsible and which it publishes, **it cannot, however, control third parties which are not expressly authorised** to process these data.

The controller's obligation to inform must therefore be **restricted to the third parties to which it has expressly given the authorisation to process these data**. Each controller's liability must be limited to its activities within its areas of responsibility.

d- The right to lodge a complaint: to be supervised

Article 73 introduces the right to lodge a complaint with a supervisory authority for any data subject or any **body, organisation or association** acting on behalf of data subjects. Furthermore, these structures may act ***independently of a data subject's complaint*** (Article 73-3).

This calls numerous principles into question: "no-one shall plead by proxy", which prevents legal action on another's behalf without having received an express mandate to do so, "authority of res judicata", meaning that the judgement is only binding on the parties present or represented in the proceedings. Furthermore, it facilitates collective redress, which have not yet been adopted at EU level.

In order not to anticipate collective redress debates, it needs to be specified that this right to complain is **limited to data subjects** and comes **within the framework of national legal provisions.** Furthermore, in order to remain compliant with the general legal principles of certain Member States, member companies recommend **removing Article 73-3.**

e- Reduction in unjustified administrative burdens: to be intensified

The Commission's proposal aims to reduce those administrative burdens which do not improve data protection. However, some of the measures proposed entail cumbersome formal obligations.

AFEP is therefore proposing:

- that the controller should ensure the **compliance of the "set of operations"**, rather than providing proof of compliance for each operation (Article 5-f);
- that the 24 hour period for notifying breaches should be replaced by a **reasonable period of time** (Article 31-1);
- that the data protection impact assessment should be replaced with an **appreciation conducted by managers in accordance with terms laid down within the company** (Article 33-1).

f- Delegated acts: to be restricted

This implementation procedure gives too much interpretative jurisdiction to the Commission, which proposes and decides almost single-handedly regarding structural matters. Furthermore, it has the effect of reducing the transparency of European legislation with regard to citizens.

Contact people:
EMMANUELLE FLAMENT-MASCARET, Director Consumer Affairs/Competition/Intellectual Property - +33 1 43 59 85 27 - concurrence@afep.com
JUSTINE RICHARD, European Affairs Deputy Director - +32 2 227 57 25 - justine.richard@afep.be