FEDERATION
BANCAIRE
FRANCAISE

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (GENERAL DATA PROTECTION REGULATION)

August 2012

The French Banking Federation (FBF) is the professional body representing the interests of the banking industry in France. Its membership is composed of all credit institutions authorised as banks and doing business in France, i.e. more than 450 commercial and cooperative banks. FBF member banks have 40,000 permanent branches in France. They employ 400,000 people, and service 60 million customers.

The FBF is in favour of the choice of legal form made by the European Commission: regulations would indeed establish a harmonised body of rules relative to the protection of personal data for all member countries.
The FBF is also in favour of the Commission's position concerning the application of the regulation to those in charge of processing who are not established in the Union, in order to avoid distortions of competition related to regulatory restrictions.
The FBF draws the Commission's attention to the necessary connection to be established between regulation on data protection and other regulations, particularly those relative to the fight against money-laundering and the financing of terrorism, in order to reconcile the growing requirements in terms of security with the key principles of the protection of personal data and personal privacy in a context of the globalisation of the economy and technologies. To this end, a study should be made on the abolition of administrative formalities with the data protection authorities concerning processing imposed by a legal obligation, as well as improved institutional cooperation between European or international bank regulators and data protection authorities, with the idea of promoting consultation and discussions so that common interpretations can be widely spread.

Key points:

- **Delegated acts**: the FBF considers that the number of delegated acts is too large and a factor in legal uncertainty.
  The FBF would like delegated acts to be abolished or incorporated into the text of the regulation itself in order to allow its immediate application through specific provisions. A delegated act may not cover an essential subject (art. 290 of the Treaty on the functioning of the European Union) with regard to the subject of the regulation. This is the case of the acts specified in articles 6, 8, 17, 18 paragraph 3, 26, 33.
  Also, a delegated act does not appear necessary when draft regulation measures are of a general nature: it is for those responsible for processing to demonstrate responsibility and to determine the appropriate resources to comply with these measures. The regulations are not intended to interfere in the organisation of companies. This is

particularly the case concerning articles 22, 23 and 31 paragraph 6 of the draft regulation.

- **Existence of sectorial provisions** (art. 17 and 18): the draft regulation is a horizontal instrument intended to apply to all sectors of activity. Yet, it transforms into general measures those that should only concern the Internet and social networks (particularly the right to data portability and the right to be digitally forgotten). The consequences of such measures, in terms of technical costs, competition risks and data-transmission security risks have not given rise to any audit or impact study.
  A limitation of the scope of the right to data portability and the right to be digitally forgotten would not weaken the protection of people who already have access and objection rights, whatever the sector of activity concerned.

- **Explicit consent** (art. 4 and 7): when the lawfulness of the processing is based on collecting consent, the draft regulation specifies that the consent must be free, specific, informed and **explicit** (which requires a positive action from the person concerned). This addition of the definition of consent is unrealistic and difficult to apply for all companies, as they have to retain their freedom and the option of setting up innovative resources concerning the procedures for collecting consent according to the vectors used (paper media, Internet and telephone) and the type of relationships established with people. It is thus necessary to come back to the definition of consent as set forth in Directive 46/95, i.e. "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*"
  Also, consent may be withdrawn by the person concerned, which has consequences that are not controlled by companies.

- **Notification of breaches of personal data** (art 4, 31 and 32): the draft regulation extends to all sectors of activity, the principle of the notification of breaches of personal data introduced by directive 2002/58/CE for the operators of electronic communications and modified in 2009, known as the "privacy and electronic communications" directive.

  All breaches of data (even the most minor) cannot be notified to the people concerned, otherwise this will create an unjustified and disproportionate climate of insecurity, confusion and anxiety. What is more, this risks generating significant costs for those responsible for processing. It is therefore necessary for any communication to people concerned, about a breach of data, to be measured and researched and not systematic.
  Also, the notification without undue delay, and if possible within 24 hours, is technically impossible to comply with and in any case would only make sense for notifications presenting a serious problem requiring quick intervention to limit the risks.

- **Data-protection officer** (art. 35): the draft regulation specifies the mandatory appointment of a data-protection officer. Creating a specific protective status of "data-protection officer" would be a source of constraints and difficulties. As a result, it is necessary to delete the following provision of article 35.7 : ""*During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties".* However, in order to ensure his/her independence, it would be necessary to associate him/her with a sufficient hierarchical level, as is the case, for example, under French law for the person responsible for compliance.

- **The one-stop shop** (art. 51): we fear that the wording of the article, if it remains unchanged, obliges groups established in several countries of the European Union to review their personal-data-protection organisation, particularly if the result of this is that the competent national data-protection authority is necessarily the one of the country where the person responsible for processing has their main establishment located. Even

for groups that have chosen to designate a single person in charge of processing for the entire group, it should not be the case that the concept of the one-stop shop necessarily results in the data-protection authority of the main establishment becoming competent to check and possibly impose penalties for any breach committed in any of the group's entities located in the European Union. Everything should depend on the nature of the shortcoming and whether or not it is related to the way the processing has been designed, when it concerns a process common to the whole of the group.
It would be more appropriate to leave international groups to decide, for each of the processes common to the whole of the group, whether they prefer to have a single person in charge of processing for the whole group or a person in charge of processing in each of the countries where the group is established.

- **Administrative sanctions** (art. 79): the draft regulation specifies the application of heavy administrative sanctions calculated from a company's worldwide revenue (until 2%), equivalent to those already existing in matters of competition. The latter are based on the negative impact of anti-competitive practices on the markets, which justifies the calculation of sanctions based on revenue.
  Such criteria of the revenue to calculate the amount of the sanctions is not relevant because non-compliance with data protection regulations harms private interests, together with individual rights, and do not harm the market.
  As a result, it is necessary that administrative pecuniary sanctions be purely standard, as it is the case for natural person responsible for the data processing in a non-commercial way (sanctions between 250,000 euros and 1 million euros maximum) and to delete the criteria of percentage of revenue.

Other general comments

- **Definitions** (art. 4): some concepts used are susceptible to interpretation because they do not correspond to legal concepts that are consistently shared at the European level. For example, it is the case with the concepts of: main establishment, enterprise, group of undertakins.
  In particular, it would be necessary to review the definition of enterprise, so that subsidiaries that do not have a corporate status are considered as companies.
  In the definition of "Group of undertakings", the concept of control should be defined by an objective criterion that is easy to determine.

- **Excessively-strict control of profiling** (art. 20): the rules proposed on profiling go far beyond those specified by the 1995 directive, which aim to reduce discriminatory behaviour having a negative impact, such as the use of automatic profiling to refuse a product or service.
  The draft regulation extends the restrictions of 1995 to practices that do not necessarily have a negative effect for people if they are intended to make information more relevant and more useful for the individual. By encompassing all forms of personalisation, whatever the possible impact on users, the new rules could compromise the effort made by companies to offer their customers "customised" products and services and degrade the quality of services offered to European citizens.

- **Reduction in formalities, but increase in obligations for those in charge of processing** (art. 28, 33 and 34): the draft regulation imposes very detailed obligations concerning the documentation of all processing performed by a person in charge of processing. These obligations appear disproportionate because they cover all processes, which will entail high costs, including for processes for which the risks are low. It would therefore be necessary to propose exceptions for this type of processing.

It does not appear necessary for the Commission to establish model forms for the documentation, because at the IT level, such documentation may be constituted in different forms left to the responsibility of those in charge of processing.

Also, the draft regulations require those in charge of processing to measure the risks presented by certain processes and to consult the data-protection authorities in case of at-risk processes.
These provisions, far from reducing administrative burden, increase them without necessarily taking into account the best practices concerning the organisation and assessment of risks put in place by those in charge of processing.
There should be no obligation to consult the data-protection authorities as long as the company has taken the necessary measures to comply with the regulations on data protection. If the principle of consultation of the data-protection authorities, and/or authorisation by them, is retained, the mechanisms should be simplified and clarified so as not to be interpreted differently by national data-protection authorities.

Furthermore, the obligation to consult the people concerned (art 33.4) should be deleted because this may harm the confidentiality of information and business secrecy. What is more, it is impossible to consult people concerning all processing or large-scale processing.

- **Class actions** (art. 73, 75 and 76): The draft regulation is not the appropriate vehicle for dealing with the question of class actions which, moreover, are the subject of general work within the European Commission in order to study the option of a Common European framework for class actions. This framework would contain a set of principles that all future EU initiatives on class actions must comply with, whatever the sector concerned.