D1391E-2012
29.10.2012

EUROPEAN BANKING FEDERATION KEY PRIORITIES REGARDING THE EUROPEAN COMMISSION PROPOSAL FOR A REGULATION ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND THE FREE MOVEMENT OF SUCH DATA

The European Banking Federation (EBF) supports the objectives of the current review. However, the European Commission's proposal aims to clarify some broad and complex issues for which the EBF identified concerns for European banks in regard to fulfilling their data protection obligations. Please find below a summary of the EBF key priorities (I) and the amendments proposed on the Regulation (II).

I. EBF KEY PRIORITIES

A. Data breach notification

Introducing an obligation to notify personal data breaches in 24 hours for other sectors than the telecommunications sectors appears disproportionate to the EBF.

At present, banks already notify their customers for instance if their credit card has been skimmed (i.e. information about a card and the associated PIN-code is copied for the purpose of manufacturing a fake card). It is also in the bank's interest to protect their customers against fraud and sustain a very high level of security. The banks can also be held liable for damages when their customers may suffer due to deficiencies in Banks IT- security systems. The banks test and update their systems and security solutions regularly to make sure that the information in the bank's system is always well-protected and secure. The transfer of information between the customer´s computer and the online banking system is always encrypted. The customer must also make sure that his/her computer, codes and personal information are protected to prevent the possibility of fraud. **To avoid "data breaches" the EBF strongly believes that it would be more effective to inform customers on how to protect their own computers, never disclose their bank account details to unknown persons etc**.

A mandatory personal data breach notification system could first give rise to organisational concerns since the implementation of such a system of notification could burden and delay the process of information to the customers.

Attention should be paid to the criteria which trigger the obligation to notify: **The notification requirement should be limited to serious breaches affecting more than one individual.** Otherwise there is a danger of triggering an avalanche of notifications with the potential to confuse and unnecessarily alarm individuals or desensitise affected data subjects (where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless).

Exemptions from data breach provisions should be awarded where sophisticated encryption is used. This will encourage the practice of encrypting personal data, especially prior to their transmission. It should also be possible to dispense with notification if measures are taken to adequately compensate those affected, e.g. by issuing new credit cards to replace cards whose details have been compromised.
A framework where notification is made in the most expedient time possible would achieve the goal of ensuring regulators and data subjects are well informed without causing unnecessary burden for regulators or alarm to victims of breaches. In addition, especially for the banking sector, notification to data subjects at all times may enable certain forms of fraud.

B. Consent

Consent given by consumers in a tacit way should be allowed. The word "explicit" should indeed be deleted as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria).

A typical consent situation within the banking industry is the transfer of data to credit agencies. This consent may under the regulation not be deemed as freely given as almost all banks require customers to sign credit agency consent. However, it is in the interest of the financial marketplace, the various financial institutions and the data subject (prevent excessive indebtedness, insolvency) to have a working credit information system.

Often customers may be perceived as being in a situation of imbalance with respect to companies that process personal data. It will be difficult to ascertain what "significant imbalance" may mean.

C. Right to data portability - Article 18

The portability principle seems to be designed for new technology / information society industry. Therefore **the EBF would like to limit the scope of Article 18 to storage of data in online-databases.** Indeed, the extension of such a right to the financial sector seems inappropriate considering the nature of the data kept in bank servers, their sensitiveness and their variety. Should the scope of this provision not be limited, we are indeed concerned that the right to data portability increases the risk of disclosure of personal data to third parties.

The EBF also would like to stress that the exercise of this right could require organisations to disclose information on trade secrets or information on other customers. The banking industry has to comply with retention requirements deriving from commercial and tax law. The obligation to bank secrecy should be taken into account.

If we take the example of a customer with a real estate loan, the data held about this customer including his financial credit worthiness represents at the same time intellectual property of the various financial institutions, which is protected by constitutional rights as well.

This principle cannot lead to a completely imbalanced between claimant and defendant in case of a civil litigation as the data subject may be in the position to extract all data from the affected company or extract at least information which would have to be provided under the very civil procedure rules.

D. Profiling - Article 20

Profiling is a typical technique used in the area of Anti Money Laundering to identify unusual financial transactions which might not fit in the financial profile of the customer. This is required by the Anti Money Laundering laws and it is also in the interest of the various financial institutions not to be misused by criminal actions. It is therefore based on the balance of interests.

It is important to stress that it might be an information overload for the customers if this information have to be given in advance of an e.g. current account contract.

In addition, as not all requirements regarding Anti Money Laundering derive from the law itself but from supervisory authority circulars we believe that it is imperative to resolve the relationship of draft regulation and the Anti Money Laundering Directive, local implementations and deduced circulars.

E. Fraud - Notably Article 6, 9, 20 and Lawfulness of processing - Article 6.1

The EBF suggests adding particular cases of lawful processing of data. The EBF considers that detecting and preventing fraud in consumer lending is of significant importance, not only to financial institutions, but can help to protect consumers from identity theft. Therefore, fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.

Banks are entitled to process fraud data in order to prevent frauds and minimise risks related to the granting of credits and undertakings. The processing of this kind of sensitive data is currently possible if data protection authorities issue permission for reason for pertaining to an important public interest. **The EBF wonders whether the restrictions of Article 9 of the proposed regulation will still allow the maintenance of such databases in the future.**

The EBF thinks that Article 6.1.c should be widened-up to include orders, recommendations of competent organisations as well as the requirements of supervisory authorities. In an on-line world and a global economy, international standards of supervisory bodies should indeed be recognised.

II. EBF AMENDMENTS

A list of proposed amendments was also presented to Members of the European Parliament (for further information, please contact advisors in charge: s.anciberro@ebf-fbe.eu & N.papp@ebf-fbe.eu).