D0208G
22/05/2012

Set up in 1960, the European Banking Federation is the voice of the European banking sector (European Union & European Free Trade Association countries). The EBF represents the interests of some 5000 European banks: large and small, wholesale and retail, local and cross-border financial institutions. The EBF is committed to supporting EU policies to promote the single market in financial services in general and in banking activities in particular. It advocates free and fair competition in the EU and world markets and supports the banks' efforts to increase their efficiency and competitiveness.

EBF POSITION ON THE EUROPEAN COMMISSION'S PROPOSAL FOR A REGULATION 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)

Key Points

The European Banking Federation (EBF) welcomes the opportunity to comment on the European Commission's proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The 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, notably on the following issues:

1. Data Breach Notification

- The EBF believes that the proposed requirement on data breach notification within 24 hours is unrealistic.
- In addition, it is important not to flood regulators with too much information which only leads to additional, unnecessary and costly burden for both the Data Protection Authorities (DPAs) and data controllers.
- Furthermore, it is important not to alarm the data subjects unnecessarily. Investigating a suspected breach generally involves a significant amount of time and effort on the part of a data controller and it can take some time to determine exactly what has happened and who is affected, with the picture often changing as the investigation progresses. There would seem to be little or no benefit in notifying a breach to a DPA before sufficient facts and the circumstances are known, to ensure the materiality of the incident is understood, unless it is obvious at an early stage that the breach has the potential to lead to significant serious harm to an individual.
- Currently the draft regulation requires a notification to the data protection authority (DPA) of all breaches of security (Article 31). With regard to the data subject (Article 32) the requirement is restricted to breaches "likely to adversely affect" the protection of the data. The EBF believes that this limitation should also apply to the notification to the DPA.
- Exemptions should be granted where appropriate measures to protect the data were applied.

a.i.s.b.l
10, rue Montoyer B-1000 Brussels
+32 (0)2 508 37 11 Phone
+32 (0)2 511 23 28 Fax

- EBF members propose that notification to a DPA should be on the same basis as for notification to an individual – when the data controller believes the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject.

2. Consent

Reliance on explicit consent and significantly restricting consent where there is an imbalance in the form of dependence between the parties creates significant complications for companies.

3. Controller and processor

- The proposed definitions of controller and processor lead to a difficult distinction of both concepts. EBF members feel that the suggested provisions add a layer of bureaucracy that goes beyond what is necessary and will not lead to improved protection for individuals.
- Current banking supervision requirements combined with the proposed requirements may overlap. Duplication of burdens should be avoided.

4. Enforcement and Penalties

Requiring penalties of up to two percent of global turnover of a business is disproportionate, particularly where the main business of the corporate is not related to personal data or data processing.

5. Delegated and implementing acts

- The present draft Regulation establishes a framework of principles. In addition to these principles, no fewer than 26 of the 91 Articles of the draft regulation give the European Commission the power to effectively adopt delegated acts.
- The EBF has serious concerns regarding this extensive power for the European Commission because of the limited involvement of stakeholders in this process.
- The EBF also sees this technique as problematic since it leaves too much uncertainty with regard to the actual implementation of the Regulation.
- This is all the most worrying as the proposed delegated acts apply to essential aspects of the draft Regulation such as the lawfulness of processing (Article 6.5), the right to be forgotten (Article 17.9), measures based on profiling (Article 20.5), data protection impact assessment (Article 33.6) etc.

6. Terminology

- Much of the terminology used in the draft Regulation is either vague or misses the opportunity to clarify long-standing terminology debates. For instance, we strongly recommend avoiding from the Regulation wording which cannot be sharply defined such as: "*verifiable consent*" (Article 8.1), "*disproportionate effort* "(Articles 12, 13 and 14).
- The EBF would expect more clarity for some key elements of the proposed Regulation.

We are grateful to be able to share our comments with you to lead to our final goal on the issue of data protection: legal certainty for the processing of banks' data.

We take the opportunity of the proposal to stress the following specific points where we think there is room for improvement.

Specific Remarks

I. GENERAL PROVISIONS

a) Legal Basis

The EBF fully understands the efforts of the European Commission to improve legal certainty and consistency by favouring a legal instrument that allows the harmonization of European data protection measures.

There are currently many inconsistencies between the provisions of national legal systems in Member States which may lead national data protection authorities to interpret the legal provisions differently. The present lack of harmonization creates substantial impediments in particular for cross-border data flows, which is very problematic for European banks. Ensuring the same level of protection to all EU data subjects is of utmost importance since it will reduce the risk of forum shopping together with the compliance burden imposed on multi-jurisdictions credit institutions.

The EBF would however welcome clarification on the relationship between some existing

i. EU legislation (e.g. the EU Consumer Credit Directive[1], the Payment Services Directive[2], the third Anti-Money Laundering Directive[3]) and the Capital Requirements Directive[4]
ii. National regulations related to data protection (e.g. in banking supervisory law related to the Capital Requirements Directive (see note 4)) and the proposed general framework.

Indeed, we wonder whether the proposed legal instrument of a Regulation will avoid overlaps which could lead to a doubling of the administrative burden, conflicts with enforcement, conflicts between supervision of privacy and financial services supervision, and problems with delineation of responsibilities and will still allow the necessary flexibility for the existence of national specificities.

Today banks are required to process personal data for a number of different reasons:

For instance, exemptions to the current European framework are granted by national data protection authorities for the maintenance of defaulters and fraudsters databases. It is to some extent necessary with sector specific legislation.

Similarly, Article 79 of the Payment Services Directive specifies that Member States shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, the investigation and the detection of payment fraud. The Consumer Credit Directive in its Article 8 describes for example a duty for creditors to assess the creditworthiness of their

[1] Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC

[2] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC

[3] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

[4] Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions, see art. 22 and annexes

customers, and it presumes that Member States have national legislation regarding credit inquiry and databases used for this purpose.

In addition, banking secrecy rules may apply in EU Member States.

Moreover , Anti-Money Laundering (AML) /Counter terrorist financing measures included in the third EU AML Directive require the processing of customers data, for instance for the application of identification obligations (Know-Your-Customer principles).

These directives often only refer to the present Data Protection Directive and do not fully analyse the consequent conflicting interests that may arise. The burden is put on the banking sector to solve any conflicting interests or to leave it up to the national authorities to interpret.

European banks would therefore need clarity as to whether the proposed general framework would still allow these specificities. We would for instance recommend the Commission to add a new article which clarifies that national law or EU law governing a specific subject matter (*lex specialis*) may override the General Data Protection Regulation.

b) Extraterritorial Scope (Article 3)

The regulation applies to companies or institutions that process personal data of individuals residing in the EU, even if the company or institution is established outside the EU. This may have important implications for businesses working within the framework of multiple jurisdictions and lead to possible legal uncertainty as data protection laws are at different stages of development across the globe.
The EBF considers it as crucial to avoid overlaps where we could face conflicting rules and inefficiencies.

c) Data subject's consent (Article 4, paragraph 8)

The EBF believes that the current definition of the data subject's consent requires more clarification. With the current requirements, the definition of consent seems to obviate the changes in technique, especially to on-line media.

More specifically, it is our opinion that the word "explicit" should 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).

II. PRINCIPLES

a) Principles relating to personal data processing (Article 5)

According to the proposed Article 5 of the draft Regulation, personal data must be limited to the minimum necessary in relation to the purposes for which they are processed (the principle of data minimization). It should be noted that this principle may be in conflict with other obligations of the banking sector, for example the proposed Directive of the European Parliament and the Council on

credit agreements relating to residential property, which requires creditors to conduct "thorough" assessment of the consumer's creditworthiness based notably on the "necessary" information (article 14); the Consumer Credit Directive (article 8) which requires creditors to assess a consumer's creditworthiness on the basis of "sufficient information" before the conclusion of a credit agreement or the Anti-Money Laundering legislation. Overlap should be avoided in this regard. The EBF believes that personal data should be proportionate to the processing purposes.

b) Lawfulness of processing (Article 6)

The EBF feels that more clarity is needed on the issue of the lawfulness of processing.

More particularly, we think that Article 6.1.c should be widened-up to include orders, recommendations of competent organizations 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 recognized.
In addition, the current formulation of Article 6.1 paragraph f is too vague to be usable.

Furthermore, we regret to note that Article 6.4 restricts the range of compatible purposes.

Finally, the power of the Commission to adopt delegated acts (Article 6.5) for this specific Article creates legal uncertainty.

c) Conditions for consent Article 7, paragraph 4

Article 7.4 will have a deep impact if it remains in its current draft. Often customers are seen to be in a situation of imbalance with respect to companies that process personal data. It will be difficult to ascertain what "significant imbalance" may mean. If one argues that customers are often in a situation of imbalance with respect to companies, consent will never be a legitimate ground to base data processing. This collides with the principle that there are six legitimate grounds for the processing of data in Article 6 (1) of the draft Regulation, consent being one of them. In addition, there are situations where data Subjects will be confronted with the choice of granting or not consent with negative consequences if they do not provide it. In these situations such choice will bring data Subjects in a situation of imbalance. This provision is likely to negatively affect the banking sector. It is arguable that banks and their customers may be in a situation of imbalance. This may lead banks not being able to rely on consent.

The banking sector is subject to worldwide heavy regulators' controls, which may require the processing of personal data for numerous specific situations. In certain circumstances, well informed consent may be the sole adequate ground for processing data in order to meet the privacy rights of Data Subjects. If paragraph 4 of Article 7 remains, the banking sector will be detrimentally affected and will be indirectly put in a situation of inequality with respect to other sectors.

In the current draft of the proposal for a Regulation, only Recital 33 attempts to clarify the meaning of 'imbalance'. In particular, it states that consent should not be considered as a valid legal ground for the processing when the data subject has no free choice and is subsequently unable to refuse/withdraw consent without suffering a detriment. Recital 34 instead of 'significant imbalance' refers to 'clear imbalance' and provides two examples of dependence, such as the employment context or when the controller is a public authority. However, these references fail, in the EBF's view, to give sufficient

clarity for the application of Article 7(4) which, as currently drafted, is likely to cause diverging interpretations and with this uncertainty. It could be that such wording is interpreted as an automatic presumption of an imbalance between the positions of the consumer and business within every single relationship.

EBF members would like to stress the importance of the legal certainty in the case of consent. Article 7 (1) already provides that the burden of proof for the data subject's valid consent is on the controller and therefore, it is in his own interest to provide for reliable means to obtain consent. What is more, should there be found that there is no sufficient legal basis for the processing or a non-compliance with Article 6, supervisory authorities shall impose a fine, to anyone who acts intentionally or negligently, up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover. Another issue which should be underlined here is the fact that the consent granted by the subject of data processing can be revoked at any time (Article 7(3)). Therefore, we do not see the need of limiting the freedom of contracts for the purpose of protecting the subjects of data processing in this manner.

Furthermore, it is a principle in banking secrecy that the customer can allow the bank to transfer his data to third parties. The new criteria "significant imbalance" could delete this principle of consent for disclosure of data.

The EBF would therefore suggest deleting the entire paragraph 4 of Article 7 or at least limiting the scope of this provision to employment contracts exclusively.

d) Special categories of personal data (Article 9)

One of our special concerns lies in Article 9 of the Regulation, which limits the right to process data related to criminal convictions and similar security measures. Under the current Directive, banks are allowed to maintain special defaulters and fraudsters databases, for which national data protection authorities may grant exemptions. These databases are used to record any frauds committed against the banks' operations. The exemption order also permits banks to disclose fraud data to other banks that are within the scope of the permission. Banks are entitled to process fraud data in order to prevent frauds and minimize 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.

We would welcome a clear distinction between data relating to criminal convictions and data relating to criminal offenses. At least the restrictions on the processing of data relating to criminal convictions should not apply to data relating to criminal offences as such restriction hampers the prevention, detection and handling of such offences.

Similarly, we notice that the processing of health/medical related data by specific sectors such as the banking and insurance sectors have not been taken into account. The EBF would support the inclusion of derogation for these specific sectors since banks and insurance companies need to process health related data in the acceptance process of some banking and insurance products. We fear that financial institutions would not be able to simply rely on the consent of the data subjects present in Article 7 when processing health/medical data because of the potential "situation of imbalance" between data subjects and financial institutions.

Similarly, we regret that Article 81 referring to the *Processing of personal data concerning health* does not cover the banking and insurance sector's groups. We believe that it is not sufficient enough to protect these sectors when providing specific services and products for which health data might be collected.

III. RIGHTS OF THE DATA SUBJECT

a) Procedures and mechanisms for exercising the rights of the data subject (Article 12)

As a general remark, we would appreciate if a clarification could be added in the Regulation to ensure that the provisions of Articles 12 to 15 on the right of access for the data subject are in line with the requirements regarding anti-money laundering and counter terrorism financing, set from the Financial Action Task Force (FATF) and implemented through the third Anti-Money Laundering (AML) Directive[5]. In particular, suspicious transactions reports submitted by financial institutions to financial intelligence units should not be disclosed to the respective person reported. The EBF fears that the present wording of Articles 12 to 15 could contradict the requirements of the Anti-Money Laundering Directive.

- **Request in electronic form: Article 12, paragraph 2:**

According to Article 12.2, the data subject may request information in an electronic form and also receive the information in an electronic form.

We acknowledge the fact that data subjects may request information electronically. However, the EBF believes that a secure way is needed to be able to provide the said data. A proper identification of the subject is needed before providing any data and to prevent any data breach possibilities.

Furthermore the data subject has to support a secure procedure for the transmission of the data via Internet, e.g. encryption mechanism.

- **Article 12, paragraph 4**

The EBF would like to stress that providing the required information implies administrative expenses (not for profit) for the banks. Therefore, the EBF considers that data controllers should be permitted to request an appropriate (not for profit) contribution in order to cover the administrative costs of providing that information. In case the Commission considers this opportunity of paramount importance the EBF would suggest limiting the free of charge only if the access is exercised once a year.

The new paragraph 4 would thus read:

> "The information and the actions taken on requests referred to in paragraph 1 shall be free of charge **once a year".**

[5] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

- **Article 12, paragraph 6**

We object to the idea of giving the Commission the mandate to lay down standard forms and standard procedures for the communication, including the electronic format. It should be up to the bank and the customer to decide on how to communicate. If the provisions are kept in the regulation some exemptions should at least be allowed for various sectors, such as the banking industry.

b) Information to the data subject (Article 14)

The EBF is also concerned about Article 14 **(1) (c)** and the responsibility to provide information on the period for which the personal data will be stored. It should be noted that the period for which the personal data is stored can be changed during customer relationship. Instead of emphasizing the requirement to inform the customer on the time period for which the data will be stored, the regulation should highlight the principle of accountability and the obligation to erase the erroneous, unnecessary, incomplete or obsolete personal data.

Additionally, the term *disproportionate effort* used in Articles 13 and 14 is open to various interpretations and it should be clarified.

c) Right of access for the data subject (Article 15)

- The EBF would welcome the restriction of the right of access for the data subject to the lawfulness of processing. We believe that recital 51 is not sufficient to ensure that the said right of access is not meant for phishing or to create a nuisance but only for the establishment of the lawfulness of the access to data. More concrete conditions for the right of access in the recitals would be welcome. We would also welcome that the concrete condition: "*be aware and verify the lawfulness of the processing*" included in Recital 51 be added to the wording of Article 15 of the draft Regulation.

- Article 15, 1, g: The EBF believes that in order to ensure legal certainty of the scope, the communication of the personal data needs to be limited. Consumers need to specify their request (time or category of data etc.) and the answer needs to be consequently proportionate.

- Article 15, paragraph 2, last sentence of paragraph 2: as mentioned previously (see remarks under Article 12, paragraph 2), the EBF believes that a secure way is needed to be able to provide the said data. A proper identification of the subject is needed before providing any data and to prevent any data breach possibilities.

d) Right to be forgotten (Article 17)

The EBF would suggest the following wording for Article 17 1(a) in order to ensure the compliance with all existing requirements in relation to data storage:

> **"**The data are no longer necessary in relation to the purposes for which they were collected or otherwise processed **and when the legally mandatory minimum retention period has expired".**

The EBF is indeed convinced that this article designed to protect internet social media users, may be extremely difficult to execute in the banking sector. Banks are obliged to store some data (e.g. for

statistics purposes to process credit applications and assess objectively the creditworthiness of customers) and therefore in the majority of cases, banks shall not be able to erase all the data processed – on request of the data subject.

e) Right to data portability (Article 18)

Article 18 applies to social networks and online-databases, where the data subject stores his personal data in an online-platform. The provision does not fit for processing of personal data in companies in their internal databases. Therefore 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.

If the scope of this provision would not be limited, we are indeed concerned that the right to data portability increases the risk of disclosure of personal data to third parties.

f) Measures based on profiling (Article 20)

We are concerned on the impact of the provisions concerning profiling to the European banking industry. The rules on profiling should not prohibit or restrict risk assessment as part of lending practices as foreseen for example in the EU Consumer Credit Directive and in banking supervisory law (risk-based approach by "Basel II")..

IV. CONTROLLER AND PROCESSOR

As a general comment on this chapter, the EBF would like to stress the fears it has of a duplication of obligations with the current proposed legislation and the current banking legislation/ requirements of the European Banking Authority (EBA). The proposed regulation adopts a rule-based approach and contains precise requirements/detailed instruction that may have a direct impact on the internal organisation of companies.

The EBF believes however that consideration should be taken of already existing obligations[6] required by financial supervision authorities on European banks in order for their internal organisation and privacy not to be put in danger by a duplication of obligations.

a) General obligations

- **Confusion between controller and processor**

The terms and corresponding liabilities of controller and processor have very often been unclear and have proven to be more and more difficult to distinguish one from another.

Unfortunately, the draft Regulation does not clarify the distinction.

[6] Consideration should be taken in particular of EBA guidelines and its 30 principles on internal governance issued in September 2011 .and Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions, see art. 22 and annexes

We would like to invite the European Commission to rethink the concepts of controller and processor. Leaving the definitions as they are, perpetuates the difficulties that in practice companies are facing when trying to comply with the data protection principles adequately. For example in the banking sector, a financial institution can be seen as controller and processor at the same time when effecting payments on behalf of their customers. Additionally, the confusion is caused by the fact that the payer partially acts as controller in respect of the payment order.

The Processor in the current times is indeed a party that processes personal data on behalf of the Controller but its knowledge about the data processing, the manner in which it chooses the means to process the data (mostly based on field knowledge and what is most cost-efficient), affect the traditional image of processors as mere instruments of the controller.

Service providers in the different sectors are traditionally viewed as "simple" processors, but in reality they have the *de facto* control on the processing of the data, not the controller.

The consequence of them being considered as "mere" processors is that it is not them upon whom the main privacy obligations fall, but still on the controller. It is therefore nor realistic nor fair that the controller primarily carries the weight of abiding by the data protection principles.

Instead of clarifying the terminology, the draft Regulation simply seems to add responsibilities to the processor. This is not considered as helpful to the data subject (who may summon one or the other party and in the end still come to the conclusion that he/she summoned the wrong one), neither does it clarifies the concepts for banks and their processors.

A solution would be to give sufficient freedom to such parties on how to best protect the privacy rights of individuals in a well established legal framework where an adequate balance between the privacy rights of individuals and the freedom to conduct a business (Article 16 of the EU Charter of Fundamental Rights) is sought. Also Article 8 of the European Convention on Human Rights (ECHR) should be taken into account when imposing obligations with respect to companies' internal organization as Article 8 of the ECHR is also supposed to protect the rights of companies.

b) Data protection by design and by default (Article 23)

With regard to the provisions regulating data protection by design and by default (Article 23), the European banking sector would strongly favour the opt-out option (default consent for data processing) in the "appropriate measures and mechanisms" to be designed by the European Commission in its delegated acts, according to paragraphs 3 and 4. This may be extremely helpful for cross-selling in banking sector.

c) Documentation (Article 28)

One of the negative consequences of the draft Regulation is the administrative burden it could imply on businesses. Article 28 introduces an obligation for controllers and processors to maintain documentation of the processing operations for which they are responsible. As stated by the EDPS in his opinion

(sections 187-189) of 7th March, the EBF doubts whether the proposed provision will lower the administrative burden.

d) Data Breach Notification (Article 31)

Financing institutions fully understand that there are circumstances that require notification to a financial and or data protection regulator in the event of a breach. Introducing an obligation to notify personal data breaches in 24 hours for other sectors than the telecommunications sectors appears however quite disproportionate to the EBF.

Article 31 introduces a general obligation for the controller to notify, where feasible within 24 hours personal data breaches to the supervisory authority and Article 32 a requirement to communicate to the data subject, without undue delay, a personal data breach which is likely to adversely affect his protection except where the controller has demonstrated to the supervisory authority that it has implemented appropriate technological protection measures and applied them to the data concerned.

Whilst the EBF understands the rationale behind the introduction of these provisions, notably enhancing both the security of processing and the accountability of the controller, we fear that the current drafting will undermine their effectiveness (as already expressed by the European Data Protection Supervisor's (EDPS) and the Article 29 Working Party's opinions on the data protection reform package, the time limit of 24 hours is unrealistic and in certain cases not feasible). Restrictions from the application of Article 32 are possible only if laid down in Union or Member State law under Article 21 of the draft Regulation.

What is more worrying, an attempt to clarify what should constitute 'adversely affect' exists currently only in Recital 66, notably a breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. Both Article 31 and 32 empower the Commission to adopt delegated acts to further specify the criteria and the requirements for establishing the data breach and the circumstances in which a personal data breach is likely to adversely affect the personal data. It is unlikely that delegated acts will be adopted at the moment when the Regulation will start to apply. Therefore the new obligations cannot effectively be implemented in the sense that, if no delegated act is in place, every single data breach will have to be notified to the national supervisory authority/communicated to the data subject. This will also have adverse consequences in the cases of imposition of administrative sanctions, notably a failure to comply with the obligation to notify a data protection breach can be fined up to 1 000 000 Euro (Article 79(6)(h)). In the absence of clear provisions ensuring legal certainty, the national supervisory authorities' practices might be highly inconsistent. Therefore, EBF is of the view that the rules regarding data breach notifications constitute essential elements of the proposal within the meaning of Article 290 of the Treaty on the Functioning of the European Union (TFEU) (Opinion shared by the EDPS and the Working Party Article 29) and should not be left to be regulated by means of delegated acts. Please find below more detailed observations regarding the content of both provisions.

At present, banks 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 their customers may suffer due to deficiencies in their 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" 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 organizational concerns since the implementation of such a system of notification could first lead to an administrative burden and in fact risk delaying the process of contacting customers when necessary. It is also important to look at the lessons learned in countries where an overlay prescriptive breach notification regime has failed to meet its objectives, and has instead created confusion and unnecessary alarm individuals, or where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless.

Should nevertheless a specific provision for data breach notification be pursued the following points should be borne in mind:

- 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. There is otherwise a danger of triggering an avalanche of notifications with the potential to confuse and desensitise affected data subjects.

- Data controllers in both the public and the private sectors should have to comply with the requirements in equal measure. From the perspective of the data subject, it is immaterial whether the breach occurred at a public institution or a private company.

- Exemptions from data breach provisions should be awarded where sophisticated encryption is utilised. 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 practice communicating data breaches to Data Subjects will often be undesirable.

For example, rights of others can be in certain circumstances negatively affected or investigations can be hindered. We observe that this Article is included in the list of articles that Member States may set aside under certain circumstances. If a data breach occurs before Member States have enacted legislation according to which this article in certain circumstances may be set aside, the obligation to inform data subjects at all times remains with all the negative effects that such notification may entail. In certain circumstances notification may hamper investigations or it may facilitate certain forms of fraud.

The obligation to notify the supervisory authority and the Data Subjects negatively affects certain sectors. The banking, insurance and telecoms sector have already specific obligations entailing the notification of such breaches to the relevant competent authorities. This would result in an unnecessary double control. In addition, especially for the banking sector, notification to Data Subjects at all times, may enable certain forms of fraud.

e) Impact Assessments (Article 33)

The draft legislation provides that prior to processing personal data, an assessment of the impact of the envisaged processing operations on the protection of personal data must be carried out. This written assessment requires consultation with data subjects. This could cause unwanted burden and costs on business with little benefit as well as an unwanted administrative burden on individuals in question.
In order to lessen the burden, consultation with data subjects should be eliminated.

f) Designation of the data protection officer (Article 35)

The task of data protection is currently cared of in a sufficient and efficient way by the compliance officer in undertakings. We know about good experiences with data protection officers in some EU Member States. But we nevertheless question the added value of a EU-wide mandatory implementation of a data protection officer. Good knowledge of data protection issues within an organisation as well as a good complaints resolution procedure is sufficient. Such a mandatory introduction could indeed lead to further administrative expenditures and not bring any added value.

V. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Articles 40-45: Representing banks operating in multiple Member States, we are grateful for the European Commission's efforts to reduce red tape around cross-border transfer of data while ensuring that subjects' data is well protected.

- **Transfer by way of binding corporate rules (Article 43)**

It is important for the EBF that not only "*controller's or processor's group of undertaking*" can use binding corporate rules (BCRs) (Article 43.1.(a)), but also cooperating financial companies, e.g. cooperation between banks and insurance companies or mortgage companies. It is indeed essential that a level playing field applies concerning the exchange of information within group companies and exchange of information between cooperating companies.

Currently organisations can rely on internal policies to make BCRs binding. However, Art. 43 explicitly requires that BCRs are legally binding. Our members suggest removing this requirement to ensure that already approved BCRs remain valid. This would also ensure that BCRs can become an effective and efficient measure for transfers or personal data and thus gain momentum as it would give organisations the flexibility how they ensure the binding nature of BCRs within their group.

VI. INDEPENDENT SUPERVISORY AUTHORITIES

a) Supervisory authority (Article 46)

Certain sectors are already subject to the supervision of sector specific regulators. In this article, reference should be made to the possibility that controllers pertaining to regulated sectors (such as the financial and insurance industry) choose to be subject to the supervision of such sector specific regulators for the observance of the Regulation. This would avoid, among others, the problem indicated in the comments regarding the notification of data breaches on double supervision.

In addition, the EBF believes that the current definition requires more clarification to avoid overlap between supervision of privacy and financial services supervision which could lead to a doubling of the administrative burden, conflicts with enforcement, problems with delineation of responsibilities, notably as regards the establishment of the fine by the competent authority.

b) Competence (Article 51)

In this article reference is made to which supervisory authority should be competent for the supervision of the processing activities. It is unclear whether the supervisory authority should be the supervisory authority of the country of the Controller or the country of Processor in the situation where Controller and Processor are not established in the same country.

In line with the EDPS' and Article 29 Working Party's opinions issued on 23rd March 2012 (page 11 and 18), the definition of main establishment and the consequences on the competences of other Data Protection Authorities (DPAs) need to be clarified. Indeed, a clear definition of 'main establishment' is crucial, as it would determine the lead authority (Article 51(2)), where 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 more than one Member State . Moreover, Recital 27 and Article 4 (13) refer to the place where main decisions as to the purposes, conditions and means of processing are taken, but does not address the situation of groups of undertakings, where several legal entities and their establishments in different countries may have a role in determining purposes, conditions and means of a processing activity, independently of the location of the central administration. This situation is addressed in the context of binding corporate rules ('BCRs') but not with regard to the definition of the main establishment (paragraph 106 EDPS's Opinion).

VII. CO-OPERATION AND CONSISTENCY

Article 66.3 requires the European Data Protection Board to publicly issue opinions, guidelines recommendations and best practices. However, Article 72 provides that the discussion of the European Data Protection Board should be kept confidential.

The current Article 29 Working Party publishes minutes of the meeting it holds. We find them very useful and would like to obtain the same transparence of the European Data Protection Board.

VIII. REMEDIES, LIABILITY AND SANCTIONS

a) Right to lodge a complaint with a supervisory authority (Article 73)

The ability for individuals to bring class actions against entities in case of negligence could have negative unintended consequence. The EBF is therefore not in favor of class actions with regard to such individual rights as privacy and data protection.. The current system containing a relevant oversight regime is sufficient according to the EBF. A one-size-fits-all approach to penalties could leave businesses facing sanctions that are too severe for the incidence in question and could hurt business in Europe in an environment that is already squeezed.

Should nevertheless class actions be accepted, the EBF believes that the representative body should evidence an interest by referring to its statutory purpose and the membership of the data subject(s), e.g. consumer organizations.

b) Administrative sanctions (Article 79)

The EBF understands that regulators currently have a large and diverse toolbox of fines, penalties and sanctions for addressing mistreatment of personal data. National regulators who are closer to their data subjects and businesses in question should have the power to create the appropriate penalties.

EBF members note the mandatory nature of the administrative sanction regime as currently drafted in the proposed Regulation. Only in some limited cases a warning may replace a sanction. What is more worrying, although Article 79(1) provides that each supervisory authority "shall be empowered" to impose administrative sanctions and Recital 120 supports this by stating that the supervisory authority "should have the power" to sanction administrative offences, Article 79(4 - 6) uses a mandatory language and states that supervisory authorities "shall impose a fine" in the situations described. This leads to a situation where very little margin of appreciation is left to the supervisory authorities. In this regard, EBF would like to stress, at the outset, the importance of the clarity and certainty of the obligations set out in the proposed Regulation (see EBF comments regarding 'consent' and 'data breach'). Having said this, EBF members believes that generally sanctions should not be systematically imposed and a margin of discretion in deciding when to impose a fine should be left to the supervisory authority since many factors influence the nature of the infringement (EDPS opinion, paragraph 266; Working Party Article 29 opinion, page 23).

As to the content of the proposed sanctions, the EBF believes that requiring penalties of up to two percent of global turnover of a business in case of data breaches is disproportionate and a principle of risk-based approach would be preferable, i.e. focusing on issues likely to create harm to individual or the society at large. EBF members feel there should be a statutory maximum figure only for fines.

IX. PROVISIONS RELATING TO SPECIFIC DATA PROCESSING SITUATIONS

X. DELEGATED AND IMPLEMENTING ACTS

a) Exercise of the delegation (Article 86)

The present draft Regulation establishes a framework of principles. In addition to these principles, no fewer than 26 of the 91 Articles of the draft regulation give the European Commission the power to effectively adopt delegated or implementing acts.

The EBF sees this technique as problematic since it leaves too much uncertainty with regard to the actual implementation of the Regulation. The effective and consistent application of the Regulation can indeed be endangered if the delegated or implementing acts are not yet adopted when the Regulation applies.

The European Data Protection Supervisor (EDPS) and the Article 29 Working Party recognizes also this point in their opinions which provide that:

EDPS' opinion of 7th March 2012 (section 71-72):
"71. In many provisions of the proposed Regulation the Commission is empowered to adopt delegated or implementing acts. Although such further acts might contribute to the uniform application of the Regulation and allow for further alignment of national practice based on experience gained after the Regulation applies, the EDPS, as said, has reservations as to an approach that builds so heavily on these acts. Furthermore, the EDPS doubts whether all issues are addressed at the correct legislative level.
72. First, if delegated or implementing acts are not yet adopted when the Regulation applies, which seems realistic with a view to the large number of envisaged acts, namely 45, the effective and consistent application of the Regulation may be at risk. For example, this could be the case with the threshold for the personal data breach notification. If no delegated act is in place, every single data breach will have to be notified to the national supervisory authority".

Article 29 Working Party opinion of 23rd March 2012 (section 'Role of the Commission', page 7) :
[…]"In practice, the adoption of delegated or implementing acts for a large numbers of articles may take several years and could represent legal uncertainty for the controllers and processors which expect implementation and concrete guidelines rapidly."[…].

Both opinions also question whether the delegated acts foreseen in the proposed Regulation are all restricted to non-essential elements as required by Article 290(1) TFEU. More specifically, essential elements should be inserted in the Regulation itself and should not be made subject to delegated acts.

Finally, the EBF would like to invite the European Commission to consult stakeholders not appointed by EU governments, including representatives of the banking sector when adopting these acts.

The EBF would favour a legislative framework addressing the above highlighted issues. This would be for the benefit of European banks and their customers whose data continue to be processed as securely as possible.

* * *

Contact persons:

Séverine Anciberro: s.anciberro@ebf-fbe.eu;
Tatyana Ferragallo: t.ferragallo@ebf-fbe.eu
Noémie Papp: noemie.papp@ebf-fbe.eu.