D2153B-2012
26.11.2012

EUROPEAN BANKING FEDERATION (EBF) POSITION ON THE JURI DRAFT OPINION ON 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 supports the objectives of the current review and welcomes the JURI draft opinion on the European Commission proposal for a General Data Protection Regulation as it rightly identified some of the key concerns for the European banking industry.

However, some provisions of the EC proposal remains to be amended and we are therefore pleased to submit to you: a summary of the EBF key priorities (I) the JURI amendments supported by the EBF (II) and the EBF amendments proposed on the Regulation (III).

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 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 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.** There is otherwise a danger of triggering an avalanche of notifications with the potential to confuse unnecessary 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).

a.i.s.b.l
Avenue des Arts 56 B-1000 Brussels
+32 (0)2 508 37 11 Phone
+32 (0)2 511 23 28 Fax

- **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 very financial institution and the data subject (prevent excessive indebtedness, insolvency) that there is 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 organizations 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 very financial institution, 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 very financial institution 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.

- Furthermore, it can be noted that the draft regulation extends the restrictions of the 1995 Directive 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. 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. Moreover, provisions on profiling need to allow profiling for legitimate interests and purposes that are for example intended to respond to consumer demands. In other words, there is no need to require additional and specific conditions for this type of profiling.

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 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.**
- The EBF thinks 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.

II. JURI AMENDMENTS SUPPORTED BY THE EBF

The European Banking Federation (EBF) welcomes the following changes which have been made to the draft text in the JURI draft opinion:

- Amendment 4 to Recital 27 containing a precise definition of main establishment is welcome for financial institutions operating in several Member States.
- Amendment 12 to Recital 67 where it is recognized that substantial breaches only should be notified.
- Amendment 13 to Recital 82 which brings clarity to the issue of the transfer of data to third countries.
- Amendment 22 to Article 4.2 bis that defines the concept of anonymous data which helps giving more legal certainty.
- Amendment 24 to Article 6.1.f where maintain the wording of Directive 95/46/EC authorises the use of third parties (e.g. credit bureaux).
- Amendment 34 to Article 15.2 which enables to verify the identity of the person requesting access in order to avoid abuses.
- Amendment 36 to Article 18 and the deletion of the right to portability which the EBF found specific to the social networks but irrelevant for the banking sector.
- Amendments 25, 29, 30, 40, 41,47, 60, 67
- Amendment 43 which helps defining clearly the information that the documentation shall contain.
- Amendment 48 to Article 31.1 which recognizes to concentrate on the measures to prevent a breach and not on minor breaches.
- Amendment 50 to Article 33 paragraph 4 which recognizes the disproportion of the EC proposal regarding the requirement of an impact assessment.
- Amendment 71 and the call for technological neutrality.

However, the EBF believes that the draft JURI opinion still requires further improvements and would strongly recommend a number of additional amendments as detailed in the attached table.

III. EBF PROPOSED AMENDMENTS TO JURI DRAFT OPINION ON THE EC PROPOSAL FOR A GENERAL DATA PROTECTION REGULATION

- Recital 25 on the conditions of consent

EC proposal	JURI amendment 3	EBF proposed amendment
(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	(25) Consent should be given explicitly by any **methods appropriate to the media used** enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	(25) Consent should be given ~~**explicitly**~~ by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent.
Justification **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) that there is a working credit information system.		

- Article 6 1. f on the Lawfulness of processing

EC proposal	JURI amendment 24	EBF proposed amendment
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks	(f) processing is necessary for the purposes of the legitimate interests pursued by a controller **or by a third party or third parties to whom the data are communicated**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, **or by the third party or parties to whom the data are disclosed** except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. **(g) the data are collected from public registers, lists or documents accessible by everyone;** **(h) the processing is necessary to defend an interest, collecting evidences as judicial proofs or file an action.**

Justification

- **The EBF agrees with the approach proposed by the draft opinion of the JURI Committee mentioning that "processing is necessary for the purposes of the legitimate interests pursued by a controller or by a third party or third parties to whom the data are communicated**". Indeed, the lawfulness of processing based on the legitimate interest must be extended to legitimate interests pursued by third parties to whom the data are disclosed by a controller as otherwise, the consequences could be to exclude the possibility for data suppliers to supply on a legitimate basis data to final users of such data even if the legitimate interest is recognized and justified.
- **In addition, the EBF suggests adding particular cases of lawful processing of data.** Processing of personal data shall be lawful if the data are collected from public registers, lists or documents accessible by everyone and if the processing is necessary to defend an interest, collecting evidences as judicial proofs or file an action.

- Article 7 on the conditions for consent (right of withdrawal)

EC proposal	JURI amendment 26	EBF proposed amendment
3. The data subject shall have the right to withdraw his or her consent **at any time**. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	-	3. The data subject shall have the right to withdraw his or her consent ~~**at any time**~~. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal **or in cases where a minimum mandatory term of storage is provided by a European or national law, or data are processed according to European and national regulatory provisions, or for anti-fraud or legal purposes. The data subject has to communicate his willingness to withdraw his or her consent to the processor. The withdrawal of the consent is effective 30 days after the receipt of the declaration.**
4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.		**4.** ~~**Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.**~~

Justification

- 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. 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. Some may argue for instance **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 to meet legal and regulatory obligations. 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 article 7.4 remains, the banking sector will be detrimentally affected and will be indirectly put in a situation of inequality with respect to other sectors.

The EBF would therefore suggest deleting the entire paragraph 4 of Article 7.

- The right of data subject to withdraw their consent at any time can actually prevent the performance of legal requirements such as those of responsible lending. It may become very difficult for financial institutions to find appropriate information in clients' databases (collecting either negative of positive information) to assess their creditworthiness when the clients may withdraw their consent whenever they feel like (for example at their very moment when their debts become overdue). The compliance with the Consumer Credit Directive Requirements (and future Mortgage Credit Directive as well) can hardly be assured and the effectiveness of creditworthiness assessment diminished.
- In the employment context, it may be appropriate that the employer can process health information concerning the employee's sick leave or data of employees covered by the collective agreements social chapters. It is also very uncertain whether an employer can process personal data concerning health at all, when the nature of art. 7, 9 and 81 is compared. If the employer cannot process health information it will complicate efforts to maintain the employee's relationship with the company and the labour market.
- It would also be extremely intrusive, if the employers no longer can process criminal records in employment. In the financial sector, it is very important that the employer is able to do so. For example, it is not reassuring that employers in connection with employment, of employees that handle the customers' money transactions, does not have the possibility to determine whether, the employee previously has been convicted of financial crimes. This process is also here governed by the general principles of treatment in Article 5 which is sufficient.
- The continued processing should be permitted in order to continue the contractual relationship that may exist between the controller and the data subject, or to allow the fulfillment of any obligation of the controller, or to respect legal basis.

- Article 12, paragraph 1, 2 and 4 Procedures and mechanisms for exercising the rights of the data subject

EC proposal	JURI amendment	EBF proposed amendment
1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular	-	1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for

mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller **shall** also provide means for requests to be made electronically.		facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller **~~shall~~ may** also provide means for requests to be made electronically.
2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. **Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.**		2. The controller shall inform the data subject without delay and, at the latest within two months of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form**,** the information shall be provided in electronic form **through a secure procedure,** unless otherwise requested by the data subject. **Before providing any data and in order to prevent any data breach possibilities**, **a proper identification of the data subject is needed.**
3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.		3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.
4. **The information and the actions taken on requests referred to in paragraph 1**		4. The information and the actions taken on requests referred to in paragraph 1 shall be

shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.		free of charge **once a year**. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

Justification

- The delay to inform the data subject is too short.
- The EBF considers that the controller should remain free to provide means to individuals for exercising their rights. 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.
- Providing the required information implies administrative expenses (not for profit) for European 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 EBF objects 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. **The EBF therefore welcomes the amendments suggested by the JURI draft opinion.**

- Article 17, paragraph 1(a) Right to be forgotten and to erasure

EC proposal	JURI amendment	EBF proposed amendment
1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available	-	1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data

by the data subject while he or she was a child, where one of the following grounds applies: **(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;** (…)		subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or **further** processed **and the legally mandatory minimum retention period has expired** (…)
Justification **The EBF is 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. For instance, for statistics purposes to process credit applications and assess objectively the creditworthiness of customers. As identified in others amendments the right to be forgotten and erasure should be limited in particular taking in consideration the data held by credit reference bureau. It should be paid attention to the misuse of this right in the field of credit. Meeting the obligations the 3rd EU Anti-Money Laundering (AML) Directive also implies the storage of data for a long period of time. Article 30 of the 3rd AML Directive provides for instance that in the case of the customer due diligence the record keeping of documents and information is required for a period of **at least five years** after the business relationship with their customer has ended. **In the majority of cases, banks shall therefore not be able to erase all the data processed – on request of the data subject.** **The term 'further processed' strikes a better balance regarding the Articles 6.4 and 5 b of the European Commission's proposal**		

- Article 20.2.c Measures based on profiling

EC proposal	JURI amendment	EBF proposed amendment
1. Every natural person shall have the right not to be subject to a **measure** which produces legal effects concerning this natural person **or significantly affects this natural person**, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health,	-	1. Every natural person shall have the right not to be subject to a ~~**measure**~~ **decision** which produces legal effects concerning this natural person ~~**or significantly affects this natural person**~~, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences,

personal preferences, reliability or behaviour.		reliability or behaviour.
2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 **only** if the processing:		2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 ~~**only**~~ if the processing:
(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or		(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or
(b) **is expressly authorized by** a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or		(b) is **necessary to comply with** ~~**expressly authorized by**~~ a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or
(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.		(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.
3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.		3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.
4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of		4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of

processing for a measure of the kind referred to in paragraph 1 **and the envisaged effects of such processing on the data subject.** **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.**		processing for a measure of the kind referred to in paragraph 1 **~~and the envisaged effects of such processing on the data subject.~~** **~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.~~**

Justification

- The EBF is concerned on the impact of the provisions concerning profiling to the European banking industry. The definition being too broad should be adapted as only decision having legal effect can be taken into consideration.
- 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 (AML) 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 AML Directive, local implementations and deduced circulars.
- Furthermore, 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"). The draft Regulation extends the restrictions of Directive 95/46 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.
- Delegated acts for this purpose are not necessary: paragraph 2 is sufficient.

- Article 79 Administrative sanctions

EC proposal	JURI amendment 63	EBF proposed amendment
3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where: (a) a natural person is processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.	3. ***The supervisory authority may give a written*** warning ***without imposing a*** sanction. ***The supervisory authority may impose a fine of up to EUR 1 000 000 for repeated, deliberate breaches or, in the case of a company, of up to 2 % of its annual worldwide turnover.***	3. The supervisory authority may give a written warning without imposing a sanction. The supervisory authority may impose a fine of up to EUR 1 000 000 for repeated, deliberate breaches ~~**or, in the case of a company, of up to 2 % of its annual worldwide turnover.**~~

Justification

- Article 79 use 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.

  The 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).

  In this perspective, the EBF is more in favor of the JURI draft opinion mentioning that "The supervisory authority may impose a fine" instead of "shall impose a fine" mentioned in the Commission's proposal and welcome the deletion of the other articles relating to the administrative sanctions.

- In addition, the EBF would like to stress that according to the subsidiarity principle usually regulation in the area of administrative proceedings and the imposition of administrative fines fall within the competences of the Member States.

  The EBF considers that the sole criteria of the annual worldwide turnover of enterprises could lead to very disproportionate amounts of fines; therefore the administrative sanctions should be limited to a fixed amount.

We hope that you will find these remarks helpful and thank you in advance for taking them into consideration for your future work on the Regulation.

Contact persons:

Séverine Anciberro: s.anciberro@ebf-fbe.eu;
Fanny Derouck: f.derouck@ebf-fbe.eu;
Noémie Papp : noemie.papp@ebf-fbe.eu