- **Right to be forgotten and to erasure**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
19.	**Article 17, paragraph 1(a)**	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 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;** (...)	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 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.

- **Right to data portability**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
20.	**Article 18**	**1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.**	1. **In cases of data stored in internet platforms of social networks,** the data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.
		2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.	~~**2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.**~~
		3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	~~**3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**~~

Justification

- **Only applicable to user generated content.**
- 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. 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 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.

- **Measures based on profiling**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
21.	**Article 20**	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, personal preferences, 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: (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	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, 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: (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	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 processing for a measure of the kind referred to in paragraph 1 **and the envisaged effects of such processing on the data subject.**	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.	~~**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.

- **Responsibility of the controller**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
22.	**Article 22**	1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article	1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1)

		34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1). 3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors. **4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.**	and (2); (e) designating a data protection officer pursuant to Article 35(1). 3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors. ~~**4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.**~~

Justification

- **The proposed definitions of controller and processor lead to a difficult distinction of both concepts. The 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** (who may summon one or the other party and in the end still come to the conclusion that he/she summoned the wrong one). 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.

  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.

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.

- **Current banking supervision requirements combined with the proposed requirements may overlap. Duplication of burdens should be avoided.**
- **Furthermore, the duplication of burdens will lead to an increase of costs.**
- The EBF would suggest deleting the provision offering the possibility for the Commission to adopt delegated act as it is up to the controller to determine the measures required to meet its obligations.

- **Sector specific supervision: new article 22b**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
23.	**Proposal for a new Article 22b**	-	**Articles 23, 26, 27, 28, 29, 30, 31, 32, 33 do not apply if and insofar as the controller is subject to a similar obligation by virtue of sector specific Union law and under supervision of an independent sectorial Supervisory Authority.**
Justification By virtue of Article 22 of Directive 2006/48/EC the national legislator may designate the Banking Supervisory Authority as the competent authority to deal with security related issues in the financial sector.			

- **Data protection by design and by default**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
24.	**Article 23**	1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and	1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures

		organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
		2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.
		3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.	~~**3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.**~~
		4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	~~**4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**~~

Justification

- The EBF would suggest deleting the provision offering the possibility for the Commission to adopt delegated act as it is up to the controller to determine the measures required to meet its obligations.
- However, should the Commission adopt delegated acts, 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.

- **Representatives of controllers not established in the Union**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
25.	**Article 25**	1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 2. This obligation shall not apply to: (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or (b) an enterprise employing fewer than 250 persons; or (c) a public authority or body; or (d) a controller offering only occasionally goods or services to data subjects residing in the Union. 3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside. **4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.**	1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 2. This obligation shall not apply to: (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or (b) an enterprise employing fewer than 250 persons; or (c) a public authority or body; or (d) a controller offering only occasionally goods or services to data subjects residing in the Union. 3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside. 4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself **as the controller remains fully liable.**
Justification Article 25 (4) implies that the representative can be held liable, while the representative should not be liable but the controller.			

- **Processor**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
26.	**Article 26**	1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.	1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.
		2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:	2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:
		(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;	(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;
		(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
		(c) take all required measures pursuant to Article 30;	(c) take all required measures pursuant to Article 30;
		(d) enlist another processor only with the prior permission of the controller;	(d) enlist another processor only with the prior permission of the controller;
		(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests	(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests

		for exercising the data subject's rights laid down in Chapter III; (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34; (g) hand over all results to the controller after the end of the processing and not process the personal data otherwise; (h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article. 3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2. 4. **If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.** 5. **The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.**	for exercising the data subject's rights laid down in Chapter III; (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34; (g) hand over all results to the controller after the end of the processing and not process the personal data otherwise; (h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article. 3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2. ~~**4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24**~~. ~~**5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.**~~
Justification			
It is the controller that instructs the processor. If the processor processes personal data other than instructed by the controller, the processor violates the agreement. Considering the processor to be a joint controller would be conflicting with the duties, responsibilities and liability of both parties and the contractual relationship between both parties.			

- **Documentation**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
27.	**Article 28**	1. Each controller and processor and, if any, the controller's representative, **shall maintain documentation** of all processing operations under its responsibility. 2. **The documentation** shall contain **at least** the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation **and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;**	1. Each controller and processor and, if any, the controller's representative, shall maintain **an overview** of all processing operations under its responsibility. 2. The **overview** shall contain ~~**at least**~~ the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation ~~**and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;**~~

		(g) a general indication of the time limits for erasure of the different categories of data; (h) the description of the mechanisms referred to in Article 22(3). 3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority. 4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities. **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.** **6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	(g) a general indication of the time limits for erasure of the different categories of data; (h) the description of the mechanisms referred to in Article 22(3). 3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority. 4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities. ~~**5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.**~~ ~~**6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**~~
Justification 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. The EBF suggests therefore deleting the word "at least" to define clearly the information that the documentation shall contain. It is not feasible to maintain documentation of all processing operations. Within the banking activities there are many processing operations. Processing of transactions alone would be impossible to document, it would mean an enormous burden on administration and archiving. It is, however, possible to maintain an overview of all the categories of processing operations.

- **Security of processing**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
28.	**Article 30**	1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. 2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data. **3. 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 the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection**	1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. 2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data. ~~**3. 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 the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default,**~~

		by default, unless paragraph 4 applies. 4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to: (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	~~**unless paragraph 4 applies.**~~ 4. The Commission may, where necessary, provide guidelines for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to: (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
Justification Depending on the type of business of the controller and the assignment to the processor appropriate technical and organizational measures may differ. It is therefore up to controller and processor to determine these measures. Guidelines may be provided by the Commission.			

- **Notification of a personal data breach to the supervisory authority**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
29.	**Article 31**	1. **In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it,** notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.	1. In the case of **any significantly harmful** ~~a~~-personal data breach the controller shall ~~**without undue delay and, where feasible, not later than 24 hours after having become aware of it**~~, notify the personal data breach to the supervisory authority **within a reasonable time.** ~~**The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.**~~ **A significantly harmful personal data breach**

			shall be determined by the controller, who can be assisted by the data protection officer, based on factors including the assessment of whether a personal data breach has created serious breaches for a significant number of data subjects. **Exemptions from data breach provisions should be awarded where sophisticated encryption is used or if measures are taken to adequately compensate those affected.**
		2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.	2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.
		3. The notification referred to in paragraph 1 must at least: (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (c) recommend measures to mitigate the possible adverse effects of the personal data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach.	3. The notification referred to in paragraph 1 must at least: (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (c) recommend measures to mitigate the possible adverse effects of the personal data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach.
		4. The controller shall document any personal data breaches, comprising the facts surrounding the	4. The controller shall document any personal data breaches, comprising the facts surrounding the

		breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose. **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.** **6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose. ~~**5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach**~~. ~~**6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**~~

Justification

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.

Furthermore, this obligation might even conflict with national financial law and regulation.

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 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" 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 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.

- The obligation to notify the supervisory authority negatively affects certain sectors. The banking, insurance and telecoms sector have already specific obligations entailing the notification of such breaches (substantial disruptions in service provided to the customers and in payment and IT system) to the relevant competent authorities. **This would result in an unnecessary double process/reporting.**
- 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.
  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.

- **Communication of a personal data breach to the data subject**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
30.	**Article 32**	1. When the personal data breach is likely to **adversely** affect the protection of the personal data or privacy of the data subject, the controller	1. **In the case of any significantly harmful personal data breach,** when the personal data breach is likely to ~~**adversely**~~ affect the protection of the

		shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. **A significantly harmful personal data breach shall be determined by the controller based on factors including the assessment of whether a personal data breach has created serious breaches for a significant number of data subjects.** **Exemptions from data breach provisions should be awarded where sophisticated encryption is used or if measures are taken to adequately compensate those affected.**
		2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).	2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).
		3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.
		4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the	4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory

		supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.	authority, having considered the likely adverse effects of the breach, may require it to do so.
		5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.	~~**5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.**~~
		6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

- A wide mandatory personal data breach notification system could give rise to organisational concerns since the implementation of such a system of notification would lead to an administrative burden and in fact risk delaying the process of contacting customers when it is really necessary (i.e. when the breach is significantly harmful)
- 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 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

- 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 Articles 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.

  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.

- 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 (Restrictions).

- **Sectorial Supervisory Authority: New Article 32b**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
31.	**New Article 32b**	-	**Articles 31 and 32 do not apply if and insofar as the controller is subject to an obligation to notify an independent sectorial Supervisory Authority by virtue of legislation based on sector specific Union law.**
Justification By virtue of Article 22 of Directive 2006/48/EC, the national legislator may designate the Banking Supervisory Authority as the competent authority to deal with security breaches in the financial sector.			

- **Data protection impact assessment**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
32.	**Article 33**	1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,	1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,

		the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
		2. The following processing operations **in particular** present specific risks referred to in paragraph 1:	2. The following processing operations ~~**in particular**~~ present specific risks referred to in paragraph 1:
		(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;	~~**(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;**~~
		(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;	(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
		(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;	(c) monitoring publicly accessible areas, **with the exception of the banking devices** especially when using optic-electronic devices (video surveillance) on a large scale;
		(d) personal data in large scale filing systems on children, genetic data or biometric data;	(d) personal data in large scale filing systems on children, genetic data or biometric data;
		(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).	(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).

		3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects **and other persons concerned.**	3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects ~~and other persons concerned~~.
		4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	~~4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.~~
		5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.	5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
		6. 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 the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	~~6. 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 the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.~~
		7. The Commission may specify standards and procedures for carrying out and verifying and	7. The Commission may specify standards and procedures for carrying out and verifying and

		auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

Data protection impact assessments 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.

- In the draft Regulation, the requirement for an impact assessment can be sanctioned by a fine of € 1,000,000 or 2% of the company's annual worldwide turnover. Considering that the wording "specific risk" is too vague and could be interpreted as limiting the requirement to only treatments listed in Article 33, deleting the word "in particular", would ensure more legal certainty.
- Processing operations' specific risks listed in 2. (a) are already mentioned and controlled by the Article 20 of this draft Regulation, it is therefore not necessary to add any additional conditions by submitting them to an impact assessment as profiling does not present any particular risks. The deletion of paragraph 2. (a) is therefore necessary.
- In order to ensure the public, the customers and the employees' security, banking activities require using optic-electronic devices (video surveillance. In these circumstances and given the specific need for the banking sector, the banking devices should be exempted from this requirement.
- In line with the justification mentioned above, the EBF suggests deleting article 33.4 as obtaining the consent of the data subject for all the processing operations requiring an impact assessment would be unrealistic leading to unreasonable charges, especially for large-scale processing operations.
- The criteria and conditions applicable to processing operations that may present specific risks, the contents of the impact assessment and the conditions of modularity, of the verification and of the auditability are key elements to be included in the regulation itself. It is therefore necessary to delete paragraph 6 related to delegated acts.

- **Designation of the data protection officer**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
33.	**Article 35**	1. The controller and the processor **shall** designate a data protection officer in **any** case where: (a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an enterprise	1. The controller and the processor **may** ~~**shall**~~ designate a data protection officer in **some** ~~**any**~~ case where: (a) the processing is carried out by a public authority or body; or

		employing 250 persons or more; or (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.	(b) the processing is carried out by an enterprise employing 250 persons or more; or (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.
		2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.	2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer. **A group of undertakings may designate a single data protection officer to deal with one or several issues implemented by several entities of the group.**
		3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.	3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.
		4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.
		5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.	5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.
		6. The controller or the processor shall ensure that any other professional duties of the data protection	6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and

		officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	duties as data protection officer and do not result in a conflict of interests.
		7. **The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.**	7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer **shall have a level of management autonomy** and may be reappointed for further terms. ~~**During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.**~~
		8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.	8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.
		9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.	9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority ~~**and to the public.**~~
		10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects shall have the right to contact the data protection officer **or any delegated officer** on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.
		11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.	11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.
Justification			
The designation of a data protection officer (DPO) as well as the working procedures of the DPO shall be subject to more flexibility than in the current EC proposal.			

- The EBF is aware of good experiences with data protection officers in some EU Member States. Nevertheless, the EBF questions 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.
- The EBF considers that in some group of undertakings some treatments may be common to different companies for transversal issues such as human resources, anti-money laundering and fight against terrorist financing, etc. In this perspective, the EBF believes that a group of undertakings might designate a single data protection officer to deal with one or several issues implemented by several entities of the group, for the group of undertakings to designate one date protection officer.
- In the EBF views, to ensure the independence of the DPO, it has to have a functional independence.
- The EBF considers the provision mentioning that "During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties" could be disproportionate and conflict with some provisions related to labour law. It may even mean, quite illogically, that for an employer there will be no chance of contract termination with a DPO for any other breach of their duties based on provision of law or contract, except for the reason stipulated above.
- The EBF believes that the contact details of the DPO should not be communicated to the public (otherwise personal data of a DPO will not be protected the same way as the data of other employees). Indeed, the EBF considers that the public have the possibility to contact the controller who will decide of the necessity to contact or not the DPO.

- **Transfers by way of binding corporate rules**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
34.	**Article 43**	1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they: **(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;** (b) expressly confer enforceable rights on data subjects;	1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they: (a) ~~**are legally binding and**~~ apply to and are enforced by every member within the controller's or processor's group of undertakings, **cooperating financial companies**, and include their employees; (b) expressly confer enforceable rights on data subjects;

		(c) fulfil the requirements laid down in paragraph 2. **2.** The binding corporate rules shall at least specify: (a) the structure and contact details of the group of undertakings and its members; **(b)** the data transfers or set of transfers, **including the categories of personal data, the type of processing** and its purposes, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both internally and externally;	~~**(c) fulfil the requirements laid down in paragraph 2.**~~ 2. The binding corporate rules shall at least specify: (a) the structure and contact details of the group of undertakings and its members; **(b)** the data transfers or set of transfers, ~~**including the categories of personal data, the type of processing and**~~ its purposes, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both internally and externally;

Justification

It is important for the EBF that not only "*controller's or processor's group of undertaking*" can use binding corporate rules (BCRs) 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, Article 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.

Article 43.2 b establishes that among other aspects BCRs should specify the data transfers or set of transfers, "including the categories of personal data" and the "type of processing". Categories of personal data and the types of processing should not be referred to in the BCRs. Making a list of these items may be contra-productive. What if new data categories of data are processed by the data controller or new types of processing are carried out with regard to the data subjects that are covered by the BCRs? Would then such data not fall within the scope of the BCRs? Would this mean that new BCRs need to be approved?

- **Derogations**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
35.	**Article 44**	1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (...) **(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or** (...) (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary. 4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers. **5. The public interest referred to in point (d) of**	1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may place only on condition that: (...) (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or **to comply with requirements of competent governmental or regulatory authorities of such third countries to which the data controller or processor is subject.** (...) (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor~~, which cannot be qualified as frequent or massive,~~ and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary. 4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers. ~~5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or~~

		paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject. **6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.**	~~**in the law of the Member State to which the controller is subject.**~~ **6. Where a transfer is based on Article 44. 1 h and the nature of the transfer or set of transfers is such that the privacy rights of the data subjects need to be adequately protected, the** controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall **consider** inform**ing** the supervisory authority of the transfer.

Justification

- It is the view of the banking sector that an exception for the disclosure of personal data to regulators or authorities of third countries to which data controllers are also subject should be explicitly referred to in the Regulation.
- **The "legitimate interest" exception**

1. The banking sector welcomes this exception, however a further analysis of this provision reveals that data controllers will hardly be able to rely on it as it is currently drafted.

2. The banking sector understands that where a data transfer is not massive or frequent such transfer is less likely to infringe the privacy rights of data subjects. To be able to rely on this ground, the banking sector proposes stipulating that any transfer based on this ground should be subject to a weighing of interests: the legitimate interest of the data controller to disclose on the one hand and on the other, the privacy rights of the data subjects. In doing so, banks should observe the principles of necessity, subsidiarity and proportionality, and adduce necessary safeguards for the transfer. These safeguards should be in syntony with the nature of such a data transfer. The banking sector is aware of the fact that documenting the steps that may lead to the disclosure contributes to making an adequate assessment of the situation. However, transfers that are less likely to affect the privacy rights of data subjects it should not be necessary to document the steps or to inform the supervisory authorities of the transfer.

3. This would cover the situation that a regulator in a third country requires once or twice (hence not frequently) specific information that could affect clients or employees of European banks, but also other possible transfers that would not be covered by the other options set out in Chapter V of the regulation. This would also cover certain disclosures to their parties in complex banking transactions where it cannot be said that the disclosure is for the benefit of the data subject and where the infringement of the privacy rights of the data subjects are unlikely to be affected, such as in securitisations or in the transfer of certain titles or claims.

4. However, it can be that due to specific legislation to which branches or subsidiaries in third countries of EU based financial institutions requires those branches or subsidiaries to provide for "frequent" disclosure of information of the EU subsidiary including individuals' related data.

5. The banking sector understands that most "massive" and "frequent" disclosures to third countries can take place either because the transfer is

effected to a country where an adequacy decision as per section 41 of the draft regulation exists, adequate safeguards as per section 42 of the draft regulation have been adopted, or where BCRs are in place as per article 43. However requests of regulators that could be qualified as "frequent" do not find a justification in the current draft Chapter V, while it would still be justified to state that a legitimate interest of the bank would exist for such "frequent" or "massive" disclosure.

6. It is the view of the banking sector that a final ground for transfers which are massive or frequent should be allowed under the Regulation. Of course, since this type of transfers are likely to infringe the privacy rights of the data subjects, the banking sector understands that adequate measures should be in place. Since banks understand the nature of the requests for disclosure, they can also assess which measures are most appropriate to respond to the protection of the individuals' right to privacy as recognised in the Regulation.

7. The Regulation's accountability principle should guarantee that the financial sector is able to decide which measures are the most appropriate when a data transfer would take place based on a "legitimate interest".

8. The most efficient way to address this is deleting the words "frequent" and "massive" and leave financial institutions with the burden of assessing themselves whether such transfer would be allowed. Financial institutions should do so based on the general principles of the Regulation such as necessity, subsidiary and proportionality and the obligation to consider the adoption of additional adequate safeguards. These may include – depending on the nature of the transfer- informing the privacy regulator.

9. Data controllers should first assess whether the transfer can be made based on other grounds. Secondly, when it has been established that this is not the case, the principles of the Regulation should be applied and an assessment should be made as to which additional measures should be taken to ensure that the privacy rights of the data subjects are adequately addressed.

- **The "public interest" exception**

1. This derogation is to be read in conjunction with Article 44.4 and 44.7 of the draft Regulation. Article 44.5 limits this derogation to the extent that it only applies where the public interest is recognised in Union law or in the law of the Member State to which the data controller is subject.

2. The banking sector believes that such public interest should also be a public interest recognised abroad. The enacting of laws abroad that provide for the disclosure of detailed banking related information responds to very specific needs of public interest [and are the product of a democratic process]. In such circumstances, banks should be able to assess the circumstances of an obligation to disclose based on the powers of a foreign regulator and weigh the privacy rights of the data subjects against the public interest at hand. The banking sector believes that the decision of disclosing such data should not be lightly made and as counterweigh, additional measures should be put in place to make such disclosure in line with the principles of the Regulation, as it should occur prior to any data processing. Any request for disclosure should be first tested against the principles of necessity, subsidiarity and proportionality. In addition and where necessary, special arrangements with the receiving party concerning the confidentiality of the data could be made.

- **Supervisory authority**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
36.	**Article 46**	1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.	1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.
		2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.	2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57. **Controllers pertaining to regulated sector should have the possibility to be subject to the supervision of such sector specific regulators for the observance of the Regulation.**
		3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Justification
Certain sectors are already subject to the supervision of sector specific regulators. Including a reference to the possibility for controllers pertaining to regulated sectors (such as the financial and insurance industry) to choose to be subject to the supervision of such sector specific regulators for the observance of the Regulation, would avoid double supervision. Indeed, 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.

- **Confidentiality**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
37.	**Article 72**	**1. The discussions of the European Data Protection Board shall be confidential.**	**1. ~~The discussions of the European Data Protection Board shall be confidential.~~ The European Data Protection Board shall make accessible its opinions, guidelines, recommendations and best practices.**
		2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.	2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.
		3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.	3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.

Justification
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.

- **Right to lodge a complaint with a supervisory authority**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
38.	**Article 73**	1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation. **2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.** 3. Independently of a data subject's complaint, any body, organisation or association **referred to in paragraph 2** shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.	1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation. ~~**2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.**~~ 3. Independently of a data subject's complaint, any body, organisation or association ~~**referred to in paragraph 2**~~ shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

Justification
• **The EBF would like to stress that the introduction of EU collective actions are still under discussion, therefore it would be more appropriate to wait for the outcome before including any such provisions in EU legislation, especially in the data protection Regulation.** The ability for individuals to bring class actions against entities in case of negligence could have negative unintended consequences. 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 organisations.

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
39.	**Article 76**	**1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.** 2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union. (...)	~~**1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects**~~. 2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union. (...)
Justification In line with the arguments developed above, the EBF would like to stress that the introduction of EU collective actions are still under discussion, therefore it would be more appropriate to wait for the outcome before including any such provisions in EU legislation, especially in the data protection Regulation. (see justifications concerning the amendment to article 73- EBF amendment 38).			

- **Administrative sanctions**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
40.	**Article 79**	**2. The administrative sanction shall be in each individual case** effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach. (...) 4. **The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:** (a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4). **5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:**	1. **Where the supervisory authority decides to impose an administrative sanction, this sanction shall ~~The administrative sanction shall be~~ in each individual case be** effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach. (...) 4. **The supervisory authority may impose a fine up to 250 000 EUR, ~~or in case of an enterprise up to 0,5 % of its annual worldwide turnover~~, to anyone who, intentionally or negligently:** (a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4). **5. The supervisory authority may impose a fine up to 500 000 EUR, ~~or in case of an enterprise up to 1 % of its annual worldwide turnover,~~ to anyone who, intentionally or negligently:**

		(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (...)	(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (...)
		6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; (b) processes special categories of data in violation of Articles 9 and 81; (...)	**6. The supervisory authority may impose a fine up to 1 000 000 EUR ~~or, in case of an enterprise up to 2 % of its annual worldwide turnover, to~~ anyone who, intentionally or negligently:** (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; (b) processes special categories of data in violation of Articles 9 and 81; (...)
		7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.	**~~7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.~~**

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 (see EBF comments regarding 'consent' and 'data breach').

  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 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.**

- **Processing of national identification number**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
41.	**Article 80a**	-	The private sector processing of a national identification number or any other identifier of general application shall not be subject to additional regulation by Member States.
Justification			
Article 8.7 of the Directive 95/46/EC provides that: "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed". The EBF would indeed like to stress that the social security number (SSN) is well spread throughout society. The SSN must be available for the purpose of structuring and organisation of large enterprise administration, increasing data quality, the faultless exchange of data between organisations en the avoidance of false hits in queries. There is therefore no justification for the current differences of approach taken by the Member States.			

- **Processing in the employment context**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
42.	**Article 82**	**1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and**	**1.** Within the limits of this Regulation, **and in particular, in accordance with the principles relating to personal data processing as set out in Article 5 and in addition to the provisions of Article 6 it shall be lawful for employers to:** **(a) process employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance**

		safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.	**of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, or rights and benefits related to employment, and for the purpose of the termination of the employment relationship; and or** **(b) install, upgrade, revise or change employee data processing systems including information technology security systems designed to protect employment data from unauthorised access by third parties, such as viruses and malware without the approval of any supervisory authority.**
		2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	~~**2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.**~~ **2. It shall be lawful for employers to transfer employee personal data referred to in paragraph 1(a) to third countries providing: the Commission has issued an adequacy decision with regard to said third country or the employer shall have in place the appropriate safeguards referred to and described in Articles 42.1 & 42.2 (b) and (c) but, in the case of employee personal data only, without any prior approval of any supervisory authority. Employers shall keep appropriate records as will enable the appropriate supervisory authorities to subsequently audit such data transfers should the need arise.**

		3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.	~~**3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1**~~ **3. Where appropriate, employers will inform employees and employees' representatives, at the relevant level, as provided for by national law and/or practice about employment related data processing activities.** **4. If an employer is found to be in breach of paragraph 2 by a supervisory authority then any enforcement notice issued against the employer by the supervisory authority shall provide the employer with days in which to remedy such breach. Any failure to remedy such breach within the required time provided in the enforcement notice will result in penalties and/or administrative fines as provided for in Articles 78 and 79.**
Justification The EBF believes that current Article 82 undermines the concept of a Regulation by allowing Member States to adopt rules additional to those already spelt out in the Regulation as regards employees' personal data. For financial institutions operating across Europe this may lead to being required to eventually comply with the Regulation and 27 different sets of domestic employment related data protection laws. Such complexity already places the EU at a competitive disadvantage in attracting employers and encouraging job growth and economic development against those world areas without such difficult and complex laws. We therefore believe that the article proposed by the EBF on the processing of employment-related personal data should replace current Article 82.			

- **Exercise of the delegation**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed

43.	**Article 86**	2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	**Deletion**

Justification

- 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.**
- A delegated act may not cover an essential subject (Article 290 of the Treaty on the functioning of the European Union) with regard to the subject of the regulation. This is the case of the acts specified in articles 6, 8, 17, 18 paragraph 3, 26, 33. Also, a delegated act does not appear necessary when draft regulation measures are of a general nature: it is for those responsible for processing to demonstrate responsibility and to determine the appropriate resources to comply with these measures. The regulations are not intended to interfere in the organisation of companies. This is particularly the case concerning Articles 22, 23 and 31 paragraph 6 of the draft Regulation.
- In their opinions, the European Data Protection Supervisor (EDPS) (section 71-72) and the Article 29 Working Party (section 'Role of the Commission', page 7) recognise also this point. 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.

***

Contact persons:

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