78

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:58
To: Verweij, Ellen
Subject: FW: Woensdag 18 december
Attachments: Themes refer to the proposed regulation as it is amended on 21 of October 2013 by LIBE committee.docx; D1391E-2012-EBF Amendments to EC Proposal for a Regulation on Data Protection 31 10 12.pdf

-----Original Message-----
From: [redacted] [mailto [redacted]]
Sent: dinsdag 17 december 2013 17:14
To: Kaai, Geran
Subject: Woensdag 18 december

Beste Geran,

Wij komen morgen graag naar de PV morgen en zullen ons om 15.00 uur melden. [redacted] is [redacted] Juridische zaken retail van de Rabobank en [redacted] is [redacted] bij ABN Amro.

Bijgesloten tref je de NVB aandachtpunten (als bijdrage voor paper van de Europese Bankenfederatie EBF) naar aanleiding van de stemming in het EP in de LIBE commissie. Omdat wij hebben samengewerkt met de EBF op dit dossier en stuur ik je voor de volledigheid ook de EBF position paper toe (ook al dateert deze uit 2012). In regel wijken onze thema's niet af van de EBF en zijn zij iets bank-specifieker dan de aandachtpunten van VNO-NCW.

Hartelijke groeten en tot morgen!

[redacted]

The following themes refer to the proposed regulation as it is amended on 21 of October 2013 by LIBE committee.

Lawfulness

Art. 6.1(f) is de basis of more than 50% of all processing operations by banks. The main reason for this is the responsibility and accountability of financial institutions for abiding by many legal obligations which are often principle based rather than of a prescriptive nature. The weighing of interests and privacy test enshrined in Art. 6.1 (f) ensures that the privacy rights of the clients of financial institutions and their employees are observed. Any restriction in comparison to the wording of article 7(f) of directive 95/46 has major impact. See connection with art. 19(2). See also connection with art. 6.1(c): when 6.1(c) is not a sufficient ground for processing banks have no alternative than relying on 6.1(f).

Art. 6.1(c): as many banking supervision law is principle based/risk based and not rule based, this legal ground is not a solid basis for all tasks carried out by financial institutions in order to comply with risk/principle based obligations. These risk/principle based obligations are set out in mandatory law of a non prescriptive nature for banks. Such legislation leaves certain room to financial institutions to decide how to fulfill such obligations. Examples of such obligations are the duty of care, checking creditworthiness and AML/combating fraud. Also pre and in-employment screening of employees cannot be based on 6.1(c).

Profiling

Art. 4(3a) defines profiling. However it makes no distinction between profiles of the personality of individuals and the outcome of algorithms that monitor deviations from average use of products in order to detect e.g. internet fraud. Such calculated average use of a product should not be confused with the profile of a personality.

Art. 19.2 has major adverse impact on regular processing operations. It disables art. 6.1(f) as legal ground for processing.

Art. 20.1: Insofar as profiling is grounded on 6.1(f) it can be forbidden under 19.2. This hinders tasks carried out by bank in order to comply with risk/principle based obligations relation to exercise of duty of care, checking creditworthiness and AML/combating fraud. Also pre and in-employment screening of employees cannot be based on 6.1(c).

Furthermore art. 20 in connection with the definition of profiling may hinder the use of detection shields in payment systems.

In addition art. 21 is amended in a manner that it does not allow the member states to tune the scope of art. 20.

Art. 5(e): reference to retention for archive purposes: however: connected to restrictive definition of 83a (archive services).

Combating fraud

Art. 9 defines special categories of data. It includes data concerning criminal or suspected offences. The processing for the purpose of prevention and detection of criminal offences is restricted in art. 9.2(j). The current room for member states to create exceptions is restricted in comparison with art. 15.5 of directive 95/46/EU.

Together with the restrictions following from articles 6.1(c), 6.1.(f) , 19.2 and 20 banks are confronted with a major problem in this area. This may imply in practice that banks cannot keep / records of clients or employees who have tried to commit or have committed fraud. Another result is that financial institutions may not be able to warn their own group members or each other on fraud activities or practices of certain individuals, with the result that it will be easier for such individuals to try "the same trick" with other financial institutions.

Foreign authorities

Art. 43a shifts the consequences of political disagreements between the EU and other nations to controllers. As a consequence of the nature of their activities banks frequently are confronted with requests for information by foreign authorities. Especially in those cases where financial institutions are also established in different countries worldwide, there is a heavy pressure to comply with of the local (financial) regulators' requests. Financial institutions will often be positioned in the dilemma of complying with the EU privacy laws or facing also important fines locally or sanctions that can involve losing the banking permit. Article 43a does not resolve the issue

Administrative burdens

Chapter IV (articles 22-37) imposes huge obligations in relation to the administrative organization of controllers. In case of banks there are many overlaps with obligations following from banking supervision legislation based on EU directives and EBA guidelines. Banks already are subject to obligations in the area of implementation of governance structures, compliance officers, security-safeguards, provision of information to the public, notification of security breaches. Banks also are subjected to double supervision.

Art. 13a and 14 establish huge obligations to inform the data subject.

Art. 17.4(da) suggests that no new systems may be implemented that for evidence purposes prohibit manipulation/erasure of data.

Art. 17.8a prescribes existence of erasure mechanisms.

Art. 33 Expansion of obligations concerning the Data protection impact assessment

European Banking Federation

D13971E-2012
29.10.2012

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

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

I. EBF KEY PRIORITIES

A. Data breach notification

- **Introducing an obligation to notify personal data breaches in 24 hours for other sectors than the telecommunications sectors appears disproportionate to the EBF.**
- At present, banks already notify their customers for instance if their credit card has been skimmed (i.e. information about a card and the associated PIN-code is copied for the purpose of manufacturing a fake card). It is also in the bank's interest to protect their customers against fraud and sustain a very high level of security. The banks can also be held liable for damages when their customers may suffer due to deficiencies in Banks IT- security systems. The banks test and update their systems and security solutions regularly to make sure that the information in the bank's system is always well-protected and secure. The transfer of information between the customer´s computer and the online banking system is always encrypted. The customer must also make sure that his/her computer, codes and personal information are protected to prevent the possibility of fraud. **To avoid "data breaches" the EBF strongly believes that it would be more effective to inform customers on how to protect their own computers, never disclose their bank account details to unknown persons etc.**
- A mandatory personal data breach notification system could first give rise to organisational concerns since the implementation of such a system of notification could burden and delay the process of information to the customers.
- Attention should be paid to the criteria which trigger the obligation to notify: **The notification requirement should be limited to serious breaches affecting more than one individual.** Otherwise there is a danger of triggering an avalanche of notifications with the potential to confuse and unnecessarily alarm individuals or desensitise affected data subjects (where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless).

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

- **Exemptions from data breach provisions should be awarded where sophisticated encryption is used**. This will encourage the practice of encrypting personal data, especially prior to their transmission. It should also be possible to dispense with notification if measures are taken to adequately compensate those affected, e.g. by issuing new credit cards to replace cards whose details have been compromised.

A framework where notification is made in the most expedient time possible would achieve the goal of ensuring regulators and data subjects are well informed without causing unnecessary burden for regulators or alarm to victims of breaches. In addition, especially for the banking sector, notification to data subjects at all times may enable certain forms of fraud.

B. Consent

- **Consent given by consumers in a tacit way should be allowed. The word "explicit" should indeed be deleted** as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria).
- A typical consent situation within the banking industry is the transfer of data to credit agencies. This consent may under the regulation not be deemed as freely given as almost all banks require customers to sign credit agency consent. However, it is in the interest of the financial marketplace, the various financial institutions and the data subject (prevent excessive indebtedness, insolvency) to have a working credit information system.
- Often customers may be perceived as being in a situation of imbalance with respect to companies that process personal data. It will be difficult to ascertain what "significant imbalance" may mean.

C. Right to data portability - Article 18

- **The portability principle seems to be designed for new technology / information society industry**. Therefore **the EBF would like to limit the scope of Article 18 to storage of data in online-databases.** Indeed, the extension of such a right to the financial sector seems inappropriate considering the nature of the data kept in bank servers, their sensitiveness and their variety. Should the scope of this provision not be limited, we are indeed concerned that the right to data portability increases the risk of disclosure of personal data to third parties.
- The EBF also would like to stress that the exercise of this right could require organisations to disclose information on trade secrets or information on other customers. The banking industry has to comply with retention requirements deriving from commercial and tax law. The obligation to bank secrecy should be taken into account.
- If we take the example of a customer with a real estate loan, the data held about this customer including his financial credit worthiness represents at the same time intellectual property of the various financial institutions, which is protected by constitutional rights as well.
- This principle cannot lead to a completely imbalanced between claimant and defendant in case of a civil litigation as the data subject may be in the position to extract all data from the affected company or extract at least information which would have to be provided under the very civil procedure rules.

D. Profiling - Article 20

- Profiling is a typical technique used in the area of Anti Money Laundering to identify unusual financial transactions which might not fit in the financial profile of the customer. This is required by the Anti Money Laundering laws and it is also in the interest of the various financial institutions not to be misused by criminal actions. It is therefore based on the balance of interests.
- It is important to stress that it might be an information overload for the customers if this information have to be given in advance of an e.g. current account contract.
- In addition, as not all requirements regarding Anti Money Laundering derive from the law itself but from supervisory authority circulars we believe that it is imperative to resolve the relationship of draft regulation and the Anti Money Laundering Directive, local implementations and deduced circulars.

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

- The EBF suggests adding particular cases of lawful processing of data. The EBF considers that detecting and preventing fraud in consumer lending is of significant importance, not only to financial institutions, but can help to protect consumers from identity theft. Therefore, fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.
- Banks are entitled to process fraud data in order to prevent frauds and minimise risks related to the granting of credits and undertakings. The processing of this kind of sensitive data is currently possible if data protection authorities issue permission for reason for pertaining to an important public interest. **The EBF wonders whether the restrictions of Article 9 of the proposed regulation will still allow the maintenance of such databases in the future.**
- The EBF thinks that Article 6.1.c should be widened-up to include orders, recommendations of competent organisations as well as the requirements of supervisory authorities. In an on-line world and a global economy, international standards of supervisory bodies should indeed be recognised.

II. EBF AMENDMENTS

- **Explicit consent**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
1.	**Recital 25**	(25) Consent should be given **explicitly** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent.	(25) Consent should be given ~~**explicitly**~~ by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent.

Justification

- With the current requirements, the definition of consent seems to obviate the changes in technique, especially to on-line media.
- **Consent given by consumers in a tacit way should be allowed. The word "explicit" should indeed be deleted** as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria).
- A typical consent situation within the banking industry is the transfer of data to credit agencies. This consent may under the regulation not be deemed as freely given as almost all banks require customers to sign credit agency consent. However, it is in the interest of the financial marketplace, the various financial institutions and the data subject (prevent excessive indebtedness, insolvency) that there is a working credit information system.

- **Consent in the case of "imbalance between the controller and the data subject"**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
2.	**Recital 34**	Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject. **However, imbalance between the controller and the data subject is not a problem where Union or Member State law has made the data subject's consent a specific condition for a specific type of processing of the personal data or set of processing operations or where the purpose or purposes of the processing of the personal data is in the interest of the data subject.**
Justification			
The imbalance should not be a problem in case the processing is required by Union or Member State law as a specific condition for the processing (other than article 6.1). E.g., the Dutch Medical Examinations Act requires employee consent for the disclosure of a medical report prepared by the company doctor to the employer. Furthermore, consent should be possible where the purpose of the processing is in the interest of the data subject. E.g., an employer should be allowed to ask the consent of an expat to disclose his personal data to a tax advisor or moving company, paid for by the employer. In this example, the tax advisor or moving company are controllers of the personal data as they render their services directly to the employee. This means that the disclosure needs a basis in article 6.1 of this Regulation. Because the use of such services cannot be made a condition of the expat contract under labour law and the disclosure cannot be based on any other processing basis as mentioned in article 6.1 except consent, the expat's consent would be required in such case.		

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
3.	**Recital 86**	Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest **laid down by Union or Member State law** so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.	Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest ~~**laid down by Union or Member State law**~~ so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients. **An important public interest may be recognised by Union or Member State Law or the law of a third country to which the data controller may also be subject.**
Justification 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.			

- **Collective redress**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
4.	**Recital 112**	(112) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge **a complaint** with a supervisory authority **or exercise the right to a judicial remedy on behalf of data subjects, or to lodge,** independently of a data subject's complaint, **an own complaint** where it considers that a personal data breach has occurred.	(112) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a **own** complaint with a supervisory authority ~~**or exercise the right to a judicial remedy on behalf of data subjects, or to lodge,**~~ **and** independently of a data subject's complaint, ~~**an own complaint**~~ where 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.

- **Scope**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
5.	**Article 2**	1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; **(b) by the Union institutions, bodies, offices and agencies;** (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; ~~**(b) by the Union institutions, bodies, offices and agencies;**~~ (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Justification

- The EBF considers that the application of the new data protection rules to EU institutions, bodies, offices and agencies should be consistent with the other legal instruments and therefore Regulation (EC) No 45/2001[1] should be fully in line with the general Data Protection Regulation. The EBF considers that the Union institutions, bodies, offices and agencies should be in the scope of the Data protection Regulation.
- The EBF believes that sufficient administrative safeguards need to be put in place to make sure that banks' clients can rest assured that the information will not be disclosed to third parties or be abused in any other way.
- The EBF would like to stress that the type of data that banks will be required to transmit to their prudential authorities (i.e. European Central bank, the Financial Stability Board located in Basel) will evolve in the future. The main objective is no longer to collect data on banks' activities in an aggregate form but also to become aware of the main bilateral links and relationships between the major financial institutions and their principal counterparties on both the assets and liability side of the balance sheet (i.e. credit exposures and funding providers). In this perspective, this means that supervisory authorities will become aware of information broken down at a contract level: top 50 individual counterparties and funding providers (single names, not aggregates) will need to be reported.

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
6.	**Article 4, paragraph 3**	(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, **consultation**, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;	(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, ~~**consultation**~~, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;
Justification			
This definition is the same as in the 95/46/EC Directive. The definition of "processing" includes the "consultation" of personal data. It seems there was no particular problem with the inclusion of the word "consultation" under the current 95/46/EC Directive. However, under the new Regulation, this means that each time a consultation is made, it is a processing in itself, thus all the requirements of the Regulation are applicable, in particular the consent of the person concerned if no other lawfulness conditions of the processing can apply. This is a problem now because tacit consent is not any longer allowed (if the name of a person is included in a database, this means normally that a previous treatment has been made, and one can rely on the fact that the person had previously been informed, or had given his consent, or the processing had been made in accordance with the applicable law…).		

[1] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Under the proposed Regulation, this means that, each time a consultation is made (such as a consultation of a bank's client name on the Internet, consultation of World Check database, consultation of the Commission's database of persons, groups and entities subject to EU financial sanctions,…), the consent of the data subject is required and he/she should also be informed of the processing. In conclusion, the word "consultation" should be deleted in the definition of "processing".

- **Definition of data subject's consent**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
7.	**Article 4, paragraph 8**	(8) 'the data subject's consent' means any freely given specific, informed and **explicit** indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	(8) 'the data subject's consent' means any freely given specific, isolated [separate – one off] **and** informed **expression of will, either by a statement or an action, which, in view of the context and circumstances at the time consent is required, signifies the data subject's agreement to the processing of the personal data** ;
Justification • Distinction must be made between isolated statements or statements as part of a contractual arrangement. • The EBF believes that the current definition of the data subject's consent requires more clarification. With the current requirements, the definition of consent seems to obviate the changes in technique, especially to on-line media. More specifically (see Recital 25), it is our opinion that the word "explicit" should be deleted as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria).			

- **Definition of personal data breach**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
8.	**Article 4 paragraph 9**	**(9) 'personal data breach' means a breach of security leading** to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of,	(9) 'personal data breach' means **a substantial** breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised

		or access to, personal data transmitted, stored or otherwise processed;	disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Justification Only substantial breaches of security should be notified in order not to represent an unnecessary burden on data protection authorities and individuals.			

- **Definition of groups of undertakings**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
9.	**Article 4, paragraph 16**	**(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;**	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings; **the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.**
Justification The EBF believes that the definition of "group of undertakings" should be clarified and include the definition proposed under Recital 28 in order to have an objective criterion for the control.			

- **Principles relating to personal data processing**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
10.	**Article 5 paragraph c**	1. Personal data must be: (...) (c) adequate, relevant, and **limited to the minimum necessary** in relation to the purposes for which they are processed; **they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does**	1. Personal data must be: (...) (c) adequate, relevant, and ~~**limited to the minimum necessary**~~ **not excessive** in relation to the purposes for which they are processed; ~~**they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that**~~

		not involve personal data; (...)	~~**does not involve personal data;**~~ (...) **2. In order to assess whether the processing of personal data for other purposes than for which the personal data was collected, is incompatible with such purposes, as referred to under paragraph 1(b), the controller shall take into account:** **(a) the relationship between the purpose of the intended processing and the purpose for which the data were obtained;** **(b) the nature of the data concerned;** **(c) the consequences of the intended processing for the data subject;** **(d) the extent to which appropriate guarantees have been put in place to protect the interests of the data subject.** **(e) the information that has been given to the data subject.**

Justification

- **It should be noted that article 5.c may be in conflict with other obligations of the banking sector**, for example the proposed Directive of the European Parliament and the Council on credit agreements relating to residential property, which requires creditors to conduct "thorough" assessment of the consumer's creditworthiness based notably on the "necessary" information (Article 14); the Consumer Credit Directive (Article 8) which requires creditors to assess a consumer's creditworthiness on the basis of "sufficient information" before the conclusion of a credit agreement or the Anti-Money Laundering legislation. Overlap should be avoided in this regard. The EBF believes that personal data should be proportionate to the processing purposes.
- In addition, the EBF considers that the **limitation of the possibility to process the personal data only if the purpose cannot be fulfilled otherwise creates the risk of litigation for banks**, either on the basis that the bank requested personal data where it is deemed unnecessary, or on the basis of not having requested all the relevant information to fully fulfill their legal obligations, be it related to Anti-Money Laundering or creditworthiness assessment.

- **Lawfulness of processing**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
11.	**Article 6**	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) **processing is necessary for compliance with a legal obligation to which the controller is subject;** (d) processing is necessary in order to protect the vital interests of the data subject; **(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;** **(f) processing is necessary for the purposes of the legitimate interests pursued by a**	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with **a EU or national** legal obligation **or legal right** to which the controller is subject **notably processing carried out on the basis of orders, recommendations of competent organizations as well as the requirements of supervisory authorities including the performance of a task carried out for assessing creditworthiness or for fraud prevention and detection purposes.** (d) processing is necessary in order to protect the vital interests of the data subject (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller **or for the performance of a task carried out for assessing creditworthiness or for fraud prevention and detection purposes;** (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, **or**

		controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	**by the third party or parties to whom the data are disclosed** except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. **This shall not apply to processing carried out by public authorities in the performance of their tasks.(g) The data are collected from public registers, lists or documents accessible by everyone;** **(g) The processing is necessary to defend an interest, collecting evidences as judicial proofs or file an action.**
		4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract. **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.**	~~**4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.**~~ ~~**5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.**~~

Justification

- The EBF suggests adding particular cases of lawful processing of data. The EBF considers that detecting and preventing fraud in consumer lending is of significant importance, not only to financial institutions, but can help to protect consumers from identity theft. Therefore, fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.
- The EBF thinks that Article 6.1.c should be widened-up to include orders, recommendations of competent organisations as well as the requirements of supervisory authorities. In an on-line world and a global economy, international standards of supervisory bodies should indeed

be recognised.

- In addition, the current formulation of article 6.1 f is too vague to be usable.
- Furthermore, the EBF regrets to note that Article 6.4 restricts the range of compatible purposes and suggests its deletion.
- Finally, the power of the Commission to adopt delegated acts (Article 6.5) for this specific article creates legal uncertainty.

- **Conditions for consent**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
12.	**Article 7, paragraph 4**	1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent **at any time**. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent ~~**at any time**~~. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal **or in cases where a minimum mandatory term of storage is provided by a European or national law, or data are processed according to European and national regulatory provisions, or for anti-fraud or legal purposes. The data subject has to communicate his willingness to withdraw his or her consent to the processor. The withdrawal of the consent is effective 30 days after the receipt of the declaration.** 4. ~~**Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.**~~

Justification

- Often customers may be perceived as being in a situation of imbalance with respect to companies that process personal data. It will be difficult to ascertain what "significant imbalance" may mean. If one argues that customers are often in a situation of imbalance with respect to companies, consent will never be a legitimate ground to base data processing. This collides with the principle that there are six legitimate grounds for the processing of data in Article 6.1 of the draft Regulation, consent being one of them.
  In addition, there are situations where data subjects will be confronted with the choice of granting or not consent with negative consequences if they do not provide it. In these situations such choice will bring data subjects in a situation of imbalance. This provision is likely to negatively affect the banking sector. Some may argue for instance **that banks and their customers may be in a situation of imbalance. This may lead banks not being able to rely on consent**.

  The banking sector is subject to worldwide heavy regulators' controls, which may require the processing of personal data for numerous specific situations to meet legal and regulatory obligations. In certain circumstances, well informed consent may be the sole adequate ground for processing data in order to meet the privacy rights of data Subjects. If article 7.4 remains, the banking sector will be detrimentally affected and will be indirectly put in a situation of inequality with respect to other sectors.

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

- The right of data subject to withdraw their consent at any time can actually prevent the performance of legal requirements such as those of responsible lending. It may become very difficult for financial institutions to find appropriate information in clients' databases (collecting either negative of positive information) to assess their creditworthiness when the clients may withdraw their consent whenever they feel like (for example at their very moment when their debts become overdue). The compliance with the Consumer Credit Directive Requirements (and future Mortgage Credit Directive as well) can hardly be assured and the effectiveness of creditworthiness assessment diminished.

- In the employment context, it may be appropriate that the employer can process health information concerning the employee's sick leave or data of employees covered by the collective agreements social chapters. It is also very uncertain whether an employer can process personal data concerning health at all, when the nature of art. 7, 9 and 81 is compared. If the employer cannot process health information it will complicate efforts to maintain the employee's relationship with the company and the labour market.
  It would also be extremely intrusive, if the employers no longer can process criminal records in employment. In the financial sector, it is very important that the employer is able to do so. For example, it is not reassuring that employers in connection with employment, of employees that handle the customers' money transactions, does not have the possibility to determine whether, the employee previously has been convicted of financial crimes. This process is also here governed by the general principles of treatment in Article 5 which is sufficient.

- The continued processing should be permitted in order to continue the contractual relationship that may exist between the controller and the data subject, or to allow the fulfillment of any obligation of the controller, or to respect legal basis.

- **Exception to Article 7 paragraph 4**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
13.	**New Article 7, paragraph 5**	-	**5. Paragraph 4 shall not apply where the data subject's consent is required:** **(a) by law, or** **(b) where the purpose of processing is likely to serve the interest of the data subject.**
Justification No consent is required in case of a processing that is necessary for the purposes of the legitimate interest 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.			

- **Special categories of personal data**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
14.	**Article 9**	1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.	**1. The processing of personal data concerning health by financial institutions shall be allowed if it is used as part of an acceptance procedure or in exercising the duty of care.** 2. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited. **(a) The prohibition as described in paragraph 2 shall not apply with respect of processing of personal data concerning criminal convictions**

			or related security measures in the context of databases which contain data on fraud committed against the credit institutions or members of other financial groups regulated by EU or national legislation and set up by financial institutions to prevent fraud. **The restrictions on the processing of data relating to criminal convictions should not apply to data relating to criminal offences.** **(b) The processing of personal data concerning health by financial institutions shall be allowed if it is used as a key factor in the assessment of risk or consumer's creditworthiness based on relevant and accurate actuarial or statistical data in the context of the provision of financial services to consumers.** **(ba) processing of data relating to criminal offences or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation or right to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.** **(bb) The prohibition to the processing of data relating to criminal convictions does not apply to responsible parties who process these data for their own purposes with a view to:**

			(bba) assessing an application by data subjects in order to take a decision about them or provide a service to them, or **(bbb) protecting their interests, provided that this concerns criminal offences which have been or, as indicated by certain facts and circumstances, can be expected to be committed against them or against persons in their service.** **The prohibition does not apply where these data are processed for the account of third parties where these third parties are legal persons forming part of the same group,**
		2. Paragraph 1 shall not apply where: (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or (...)	**3. Paragraph 2** shall not apply where: (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or (...)

Justification

- Under the current Directive, banks are allowed to maintain special defaulters and fraudsters databases, for which national data protection authorities may grant exemptions. These databases are used to record any frauds committed against the banks' operations. The exemption order also permits banks to disclose fraud data to other banks that are within the scope of the permission.

- Banks are entitled to process fraud data in order to prevent frauds and minimize risks related to the granting of credits and undertakings. The processing of this kind of sensitive data is currently possible if data protection authorities issue permission for reason for pertaining to an important public interest. **The EBF wonders whether the restrictions of Article 9 of the proposed regulation will still allow the maintenance of such databases in the future.**
- We would welcome **a clear distinction between data relating to criminal convictions and data relating to criminal offenses. At least the restrictions on the processing of data relating to criminal convictions should not apply to data relating to criminal offences** as such restriction hampers the prevention, detection and handling of such offences.
- As regards to health data, the EBF would support the inclusion of derogation for these specific sectors since banks and insurance companies need to process health related data in the acceptance process of some banking and insurance products. We fear that financial institutions would not be able to simply rely on the consent of the data subjects present in Article 7 when processing health/medical data because of the potential "situation of imbalance" between data subjects and financial institutions.

- **Definition of personal data concerning criminal convictions**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
15.	**Proposal for a new Article (12a)**	-	**(12a) 'personal data concerning criminal convictions' means any personal data relating to the application of the criminal justice system;**
Justification			
Controllers that are victim of criminal offences should have the right to process data of such offences committed against them or their organisations.			

- **Procedures and mechanisms for exercising the rights of the data subject**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
16.	**Article 12**	1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms	1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms

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

		burden of proving the manifestly excessive character of the request. **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 the manifestly excessive requests and the fees referred to in paragraph 4.** **6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	burden of proving the manifestly excessive character of the request. ~~**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 the manifestly excessive requests and the fees referred to in paragraph 4.**~~ ~~**6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**~~

Justification

- The delay to inform the data subject is too short.
- The EBF considers that the controller should remain free to provide means to individuals for exercising their rights. We acknowledge the fact that data subjects may request information electronically. However, the EBF believes that a secure way is needed to be able to provide the said data. **A proper identification of the subject is needed before providing any data and to prevent any data breach possibilities. Furthermore the data subject has to support a secure procedure for the transmission of the data via Internet**, e.g. encryption mechanism.
- Providing the required information implies administrative expenses (not for profit) for European banks. Therefore, **the EBF considers that data controllers should be permitted to request an appropriate (not for profit) contribution in order to cover the administrative costs of providing that information.** In case the Commission considers this opportunity of paramount importance the EBF would **suggest limiting the free of charge only if the access is exercised once a year.**
- The EBF objects to the idea of giving the Commission the mandate to lay down standard forms and standard procedures for the communication, including the electronic format. It should be up to the bank and the customer to decide on how to communicate.

- **Information to the data subject**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
17.	**Article 14**	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (a) the identity and the contact details of the controller **and, if any, of the controller's representative and of the data protection officer;** (b) the purposes of the processing for which the personal data are intended, **including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);** **(c) the period for which the personal data will be stored;** (...) 5. Paragraphs 1 to 4 shall not apply, where: (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a **disproportionate effort**; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (a) the identity and the contact details of the controller ~~**and, if any, of the controller's representative and of the data protection officer**~~; (b) the purposes of the processing for which the personal data are intended, ~~**including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);**~~ ~~**(c) the period for which the personal data will be stored;**~~ (...) 5. Paragraphs 1 to 4 shall not apply, where: (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve ~~**a disproportionate effort**~~ **difficulties**; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by

		(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.	law; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

Justification

- It is suggested that the data subject addresses his/her request to the service in charge (a delegate to the data protection in the company) but not to a natural person (Mr. or Ms. X) responsible for this particular function. A change in the name of the person in charge would indeed imply a change in all the contractual documentation containing his/her name.
- It should be noted that the period for which the personal data is stored can be changed during customer relationship. Instead of emphasising the requirement to inform the customer on the time period for which the data will be stored, the regulation should highlight the principle of accountability and the obligation to erase the erroneous, unnecessary, incomplete or obsolete personal data.
- The EBF considers the term "disproportionate effort" opens to various interpretations and should be clarified.
- The proposed Regulation requires the provision of a specific explanation of the justification for processing data (under Art 14, b, Art 15, h). Given that the rationale behind the processing of data is usually very clear to customers, (e.g. when applying for a mortgage or a bank account), the benefits associated with justification of processing in all circumstances are questionable. We would suggest the deletion of the above words in Article 14(1) (b

- **Right of access for the data subject**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
18.	**Article 15**	**1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:** (a) the purposes of the processing;	1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed **in order to be aware and verify the lawfulness of the processing**. Where such personal data are being processed, the controller shall provide the following information: (a) the purposes of the processing;

		(b) the categories of personal data concerned; (c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries; **(d) the period for which the personal data will be stored;** (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; **(g) communication of the personal data undergoing processing and of any available information as to their source;** (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20. **2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.**	(b) the categories of personal data concerned; (c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries; **(d) ~~the period for which the personal data will be stored;~~ A general indication of the period of time for which the personal data will be stored. The data controller must provide more detailed retention periods if requested by the data subject.** (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (g) communication of the personal data undergoing processing and of any available information as to their source **if the request is specified with clear criteria such as the time or the category of data;** (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20. 2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing **in order to be aware and verify the lawfulness of the processing**. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, **through a secure procedure,** unless otherwise requested by the data subject. **Before providing any data and in order to prevent any data breach possibilities, a proper identification of the subject is needed.**

		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 communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1. 4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	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 communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1. 4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

The EBF would welcome the restriction of the right of access for the data subject to the lawfulness of processing. We believe that recital 51 on competence is not sufficient to ensure that the said right of access should not be used for vexatious purposes or as part of a fishing expedition in the preparation of a law suit, but only for the establishment of the lawfulness of the access to data. More concrete conditions for the right of access in the recitals would be welcome. We would also welcome that the concrete condition: "*be aware and verify the lawfulness of the processing*" included in Recital 51 be added to the wording of Article 15 of the draft Regulation.

- Article 15, 1, g: The EBF believes that in order to ensure legal certainty of the scope, the communication of the personal data needs to be limited. Consumers need to specify their request (time or category of data etc.) and the answer needs to be consequently proportionate.
- Article 15, paragraph 2, last sentence of paragraph 2: as mentioned previously (see remarks under Article 12, paragraph 2), the EBF believes that a secure way is needed to be able to provide the said data. A proper identification of the subject is needed before providing any data and to prevent any data breach possibilities.
- The proposed Regulation requires the specific period for the retention of personal data to be relayed to the customer (Art 15, d). Given that different data will have different retention periods, it may be challenging for customers to view this information on a privacy notice. Provided that the business complies with existing obligations to retain data for as long as is necessary, this should satisfy the data protection requirements. It is therefore difficult to see how specifying a retention period for different types of data would necessarily benefit the customer.