EACB comments on the European Commission Proposal for the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data – General Data Protection Regulation (GDPR)

26 April 2012

The EACB is the voice of the co-operative banks in Europe. It represents, promotes and defends the common interests of its 28 member institutions and of co-operative banks in general. Co-operative banks form decentralised networks which are subject to banking as well as co-operative legislation. Democracy, transparency and proximity are the three key characteristics of the co-operative banks' business model. With 4.200 locally operating banks and 63.000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 160 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 50 million members and 750.000 employees and have a total average market share of about 20%.
For further details, please visit http://www.eurocoopbanks.coop/

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eurocoopbanks.coop • e-mail : secretariat@eurocoopbanks.coop

The European Association of Co-operative Banks (EACB) takes note of the Commission proposal for the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data – General Data Protection Regulation (2012/0011 (COD)), and would like to comment on its selected provisions.

1. Legal form of legislation

In the Explanatory Memorandum to its Proposal[1] for Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Regulation, GDPR), the Commission argues that the analysis of subsidiarity principle, as described in Art 5(3)TEU, indicates the necessity of EU-level action. A regulation is considered to be the most appropriate legal instrument for the new data protection framework. The EACB recognises the reasoning for the implementation of new EU-wide data protection standards, and in this context would like to recall that the aim of the proposal was to create clear and common rules, which would enhance the legal security and minimize red tape. In such context, the EACB would be in principle supportive of a directly enforceable regulation which would allow avoiding gold plating by the Member States, a problem that had been experienced in many countries under the regime of the current Directive 95/46/EC. However, having analysed the current Commission proposal for the regulation, the EACB is concerned that, on the contrary, the proposal in its current shape would significantly increase the costs in IT-systems and unjustly increase the red tape in general.

In should be recognised that any proposals that are made on top of the existing data protection legislation will have a significant impact on the financial industry. All new changes affect very deeply every single actor in the financial market, and the EACB would recommend bearing in mind the special characteristics of the financial sector. Financial market is highly regulated with a wide range of stringent provisions, and therefore there is an increased risk of overlapping regulations if the specificities of the financial sector are not properly taken into account.

Information technology in the individual Member States is still on a different technical level. In addition, there are already a large number of national laws and regulations in this field. Differences in the circumstances of national markets and also different cultures should be kept in mind when considering new legislation. For example, a directive would leave each Member State the decision as to whether the fundamental right to data protection should be confined to natural persons only, or whether it should also protect legal entities[2]. Thus, the EACB would invite to further reflection on whether the objectives set out for the data protection review could be better achieved by way of a directive rather than a regulation. Nevertheless, should it be decided that the regulation is indeed the most appropriate tool, the EACB would strongly recommend improvements which are necessary to meet the intended goals of a regulation, including finding appropriate solutions to a number of conflicts that are likely to arise:

- The relationship of the regulation with the existing data protection legislation in other EU legislative acts, e.g. in the Directive 2008/48/EC on credit agreements for consumers (CCD), or the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (AML Directive);
- An opportunity to flesh out the regulation by national legislation or continued existence of national special regulations (e.g. national regulations for credit bureaus,

[1] c.f. Section 3.1 "Legal Basis"
[2] as this is presently the legal situation in Austria, Italy, Denmark and Luxemburg

prudential norms for money laundering, corruption and anti-fraud, prudential rules for scoring, data protection legislation in the field of Telemedia); and
- The relationship with the applicable legal regulations in some Member States for banking secrecy.

2. Definitions

The EACB would like to put forward the following suggestions concerning the definitions included in the Article 4 of the regulation proposed by the Commission:

- In the definition of a 'recipient' (Art 4(7)), the EACB would recommend defining more clearly the phrase *'personal data are disclosed'* since there are many different types of situations where personal data can be legally handed over; In fact, the terms 'disclosed' and 'transferred' and the difference between the two, should be in our view clearly defined in the new Regulation;
- The definition of 'the data subject's consent' in Art 4(8) should in our opinion also include a consent given by the consumer in a tacit way; in this context, the EACB would also recommend deletion of the word 'explicit' from Recital 25;
- Finally, the interpretation of a 'group of undertakings' in Art 4(16) as a controlling undertaking and its controlled undertakings seems to be too narrow and the EACB would recommend expanding it to all financial groups recognised by the legislation, including co-operative groups and financial conglomerates.

COM proposal	EACB proposal
Article 4 (7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed; _____ (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; *[related issue]* ***Recital 25*** Consent should be given ***explicitly*** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or	Article 4 (7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed ***or transferred***; _____ (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; ***this also includes a consent given by the consumer in a tacit way;*** *[related issue]* ***Recital 25*** Consent should be given ~~***explicitly***~~ by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or

purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
_____	_____
(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	***(16) 'group' means the group of undertakings consisting of a parent undertaking and its subsidiaries within the meaning of Articles 1 and 2 of the Seventh Council Directive 83/349/EEC of 13 June 1983 on consolidated accounts or the group of undertakings referred to in Article 3(1) and Article 80(7) and (8) of Directive 2006/48/EC[3] and other financial groups regulated by EU or national legislation;***

3. Significant increase of controller's duties

Although the Commission proposed the new regulation in pursuit of freeing up businesses from unnecessary and burdensome technicalities, the EACB believes that actually there is a significant increase of duties imposed on controllers by virtue of Articles 12, 14, 15, 17, 18, 28, 31 and 32. In fact the EACB is concerned that those extra duties would be difficult to implement and would no doubt lead to additional red tape. They would also lead to an expansion of the information requirements and to an information overload. The EACB would like to strongly recommend ensuring that excessive formalization and bureaucracy are avoided.

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

This Article provides for numerous obligations for controllers to establish procedures and mechanisms for:

- providing the information by the consumer to the controller for the purpose of rectification of the personal data relating to them; informing the data subject whether, and if so, how, why and for how long his personal data are being processed;
- exercising by the data subjects their rights to be forgotten and the right to erasure, right to data portability, right to object, 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 on automated processing (profiling measures),
- electronic requests, responses to the data subject's request within a defined deadline, and the motivation of refusal, and
- ensuring and being able to demonstrate that the processing of personal data is performed in compliance with the GDPR.

The EACB would strongly recommend deletion of Paragraph 1 of Article 12 which we consider to be superfluous.

Concerning Paragraph 2, it should be pointed out that the fact that data are processed automatically does not necessarily mean that the company also has the technical means

[3] Or *"Article 9, Article 108(6) and Article 108 (7)"* [as inserted by OP i.e. new Capital Requirements Regulation]

to provide information in the same way. This requirement would pose considerable additional expenses, in particular for small and medium enterprises. Thus, it should be within the discretion of the controller to decide in what form he provides the information in question. In addition, safety aspects also speak against electronic provision of information. This relates to the fact that the identification of the person requesting the information may not be possible and thus the security of data transmission cannot be ensured.

In paragraph 2 it is not clear what an 'electronic form' means exactly, and therefore the EACB would recommend deleting a reference to it in the current form.

Finally, further specification of the criteria and conditions for the manifestly excessive requests and the fees should not, in our view, be transferred to the Commission, and - if necessary - should rather fall under the full-fledged legislative process,. Likewise, the EACB is strongly opposed to standardisation of forms and procedures, the development of which should remain with controllers.

COM proposal	EACB proposal for amendment
1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular 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.	~~***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.***~~
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 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.***~~
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	4. The information ***referred to in Article 14*** and the actions taken on requests referred to in ~~***paragraph 1***~~ ***Article 13 and Articles 15–to 19*** shall be free of charge. Where requests are manifestly excessive, in particular because of

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.	their repetitive character, the controller ***shall be entitled to exercise its right pursuant to paragraph 3 or*** 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.	~~***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).	~~***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).***~~

3.2. Information to the data subject (Article 14)

This article introduces a significant increase in information duties of a controller vis-à-vis the data subject (Art 14). In particular, this extensive information - which is to be provided automatically and without request - must be provided also when the personal data is not collected but it originates from a different source.

The provision of such extensive information in every case seems to present a disproportionate effort. This, to some extent, is recognised in Article 14(5)(b) which states that the information requirements shall not apply where *"the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort"*. The EACB members consider that it should be sufficient that the data is available and easy to collect. Therefore we would suggest that the provision of following information, via the internet or at the bank branches, would suffice:

- The name and contact details of the controller;
- The purpose of the processing for which the data are intended (in line with Art 10(b) of the Directive 95/46/EC on data protection); the EACB believes that the obligation to notify to the client the general contract terms and conditions is already regulated in the civil law and is therefore not to be determined by data protection law; In addition, we wish to stress that in case of point (b) of Article 6(1) the data subject will already have the knowledge of the contract terms and general conditions. With respect to point (f) of Article 6(1), the contractual relationship (and thus the terms and conditions) will as a rule only exist between the controller and a party other than the data subject;
- At the outset of the relationship, it is not possible to inform clients about the duration of the storage of the data because it is not foreseeable how long the business relationship would last; this is particularly true in the banking industry with "continuing obligations". In addition, under Article 30 of the AML Directive, documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing must be kept by banks for a period of at least five years after the business relationship with their customer has ended. The same term

of five years is envisaged in Article 5(5) of the Regulation 1781/2006 on information on the payer accompanying transfers of funds;

- Where the data subject has already a legal right of request, there is no added value in informing him about those rights; the EACB would like to emphasise its recommendation to avoid information overload for the data subjects;
- The information could not be given in the flow of international payments and international securities business.

Finally, the EACB calls for due consideration for specific cases where operations requiring significant transfer of personal data take place.

COM proposal	EACB proposal
1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:	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;***	(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);***	(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;	~~***(c) the period for which the personal data will be stored;***~~
(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;	~~***(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;***~~
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;	~~***(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;***~~
(f) the recipients or categories of recipients of the personal data;	(f) the recipients or categories of recipients of the personal data;
(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;	~~***(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;***~~
(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.	(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.
2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences	2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences

of failure to provide such data. 3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate. 4. The controller shall provide the information referred to in paragraphs 1, 2 and 3: (a) at the time when the personal data are obtained from the data subject; or (b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed. 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 (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.	of failure to provide such data. 3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate. 4. The controller shall provide the information referred to in paragraphs 1, 2 and 3: (a) at the time when the personal data are obtained from the data subject; or (b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed. 5. Paragraphs 1 to 4 shall not apply, where: (a) the data subject already has 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 (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. ***6. In case of an operation that requires significant transfer of personal data, including operations of merger and acquisition, sale of entities or their part, transfer of going concern, securitisation, or block of credit sale, the assignor shall provide data subjects with the information mentioned in paragraphs 1 to 4 at the first available occasion after the transfer/sale has taken place.***

3.3. Right of access for the data subject (Article 15)

This provision envisages very extensive obligations for the controller in the context of the right of access for the data subject.

The EACB would recommend clarifying that the claim could only be used for purposes of data protection rights and not for a general 'fishing expedition claim'. The EACB is opposed the obligation of the controller to provide the data subject with information about the existence of legal claims the data subject can make in the context of a contractual relationship.

The EACB would also recommend deletion of paragraph 3 which allows the Commission to specify the criteria and requirements for the communication to the data subject of the content of the personal data. We strongly believe that regulation of those details should

not be delegated to the Commission. Certain level of flexibility should be ensured to address the needs of specific situation, and we would rather recommend the introduction of provisions limiting the right of information, particularly in relation to trade secrets and proprietary rights of the person responsible (this is partially recognised in the recital 51 of the proposed regulation, where it is stated that *"This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software"*).

The development of forms should in our opinion be left to the discretion of the controllers, as standardisation would lead to additional red tape.

COM proposal	EACB proposal
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; (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. ***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***	1. The data subject shall have***, for the performance of his rights under this regulation,*** 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; (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. ~~***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***~~

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).	~~***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).***~~

3.4. Right to be forgotten and to erasure (Article 17)

This article provides the data subject with the right to be forgotten and to erasure. This does not take into account the special demands and characteristics of financial institutions. It is very important that the right to be forgotten does not preempt the controller to act in situations where he has a clear and legal reason to have also data from clients who no longer have a client relationship with the institution (i.e. relating to guarantees, debt collection, etc.). For example, the requirements of keeping the relevant data for at least five years after the business relationship with their customer has ended under the AML Directive and Regulation (EC) 1781/2006 should not be overlooked.

In addition, it is not for the controllers to consider the objectives of the national law, and therefore we would strongly recommend modifying point 3(d) accordingly.

COM proposal	EACB proposal
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 (…) 3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; ***Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;*** (e) in the cases referred to in paragraph 4. 4. Instead of erasure, the controller shall restrict	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, ***and all the obligations of the controller and the data subject resulting from the contractual relationship between them have been fulfilled, and the controller is not under a legal obligation, be it under the EU or national legislation, to keep the data after the contractual relationship between the said controller and the data subject has expired.*** (…) 3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member

processing of personal data where: (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; (d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2). 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest. 6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing. 7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed. 8. Where the erasure is carried out, the controller shall not otherwise process such personal data. ***9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:*** ***(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;*** ***(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;*** ***(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.***	State law to which the controller is subject***, including secondary regulations of national authorities***; ~~***Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;***~~ (e) in the cases referred to in paragraph 4. 4. Instead of erasure, the controller shall restrict processing of personal data where: (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; (d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2). 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest. 6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing. 7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed. 8. Where the erasure is carried out, the controller shall not otherwise process such personal data. ~~***9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:***~~ ~~***(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;***~~ ~~***(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;***~~ ~~***(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.***~~

3.5. Right to data portability (Article 18)

The EACB appreciates that this provision may be useful in the context of, for example, social networks, where the data subject may wish to transfer the data from one network to another. However, this provision is not appropriate in case where the data controller is a bank. We would therefore propose limiting the scope of this provision to social networks.

Paragraph 3 of Article 18 states that the Commission is empowered to specify the electronic format and the technical standards, modalities and procedures for the transmission of personal data. The article raises issues relating to standardization and has potential cost implications for businesses, especially relating to changes in the data systems. Additional costs may be caused, for example, by the fact that there is not any single platform in IT systems which would allow giving and receiving data in a 'commonly used format'. Finally,determining the electronic format by the Commission would mean a substantial interference with the constitutionally protected freedom of business organization.

Careful consideration needs to be also given as to whether 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 duly taken into account.

Finally, the EACB evaluates this proposal negatively from the point of copyright protection of databases. Compatibility of this provision with Directive 96/9/EC on the legal protection of databases should be carefully considered. In terms of the type of data that should be transmitted, it is not clear whether this would cover the data that were provided by the data subject, or whether this would also include the results of the processing of this data, in which case this would not be compatible with Article 7 of the Directive 96/9/EC according to which *"Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database".*

COM proposal	EACB proposal
1. ***T***he 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.*** ***3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities***	1. ***If t***he data subject ***puts personal data in a social network, 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.***~~ ~~***3. The Commission may specify the***~~

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).	~~***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).***~~

3.6. Documentation (Article 28)

This provision introduces new and very extensive documentation requirements, which would pose significant additional red tape. In this context, the EACB would like to propose several adjustments.

COM proposal	EACB proposal
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;*** (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	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; (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).***	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).~~***

3.7. Security of processing and notification of a personal data breach (Articles 30 and 31)

This Article introduces an obligation for the controllers to notify the supervisory authorities of any personal data breach within 24 hours from the moment the controller becomes aware of it. In addition, Article 32 requires the controller, after the notification to the supervisory authority is made, to communicate a personal data breach to the data subject when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject.

It is the view of the EACB that data breach notifications should be limited to the most harmful breaches. The harm that a personal data breach creates for a large number of individuals should be one of the main criteria triggering the obligation to notify. If companies have to notify data breaches for which the risk of harm is limited, the benefit for individuals would be also limited and it would create disproportionate administrative costs for companies and possible damages to their reputation even when there is no real consumer detriment. For example, the notification requirement should not apply if the loss of data poses no threat because the data were properly encrypted. The assessment of the seriousness of data breaches could be left to the processor assisted by the data protection officer (if the company appoints one).

COM proposal	EACB proposal
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. 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	1. In the case of a ***significantly harmful*** 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.~~*** ***1a. 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 harm for a significant number of data subjects.***

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 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).	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. 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).

3.8. Data protection impact assessment (Article 33)

With reference to the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations, the EACB appreciates the intention to consider specific measures for small, medium and large entities (SMEs) when adopting delegated acts for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks (as envisaged in Paragraph 6 last sentence of Article 33). In this context, the EACB would suggest using the UE criteria defined in the Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises, in particular to define SMEs.
Furthermore, the EACB would suggest modifying point 7 of article 33 as proposed below.

COM proposal	EACB proposal
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).	7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3, ***including the use of a common format, for all the member states, that the data controller shall draw up, containing appropriate information with regard to the assessment taken.*** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

4. Other issues

4.1. Collective redress (Recital 112)

The question of the introduction of EU collective action, including representative actions by interest groups, is still being debated by EU policy makers. The EACB would thus recommend waiting for the results of those considerations before including any such provisions in EU legislation dealing with more specific elements, such as data protection. The EACB agrees with the conclusions of the ECON Committee in its 2011 draft report on collective redress[4] that *"any proposal in the field of collective redress should take the form of a horizontal instrument."* We do not consider that introducing separate provisions specific to the legal basis of a judicial claim is the right approach.

COM proposal	EACB proposal
Any body, organisation or association which aims to protect***s*** 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.	Any body, organisation or association which aims to protect~~s~~ 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 ***and~~or exercise the right to a judicial remedy on behalf of data subjects~~*** independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.

4.2. Processing by Union institutions, bodies, offices or agencies (Art 2(2)(b))

The present Art 2(2)(b) indicates that the proposed regulation shall not apply in general to the processing of personal data by the Union institutions, bodies, offices and agencies. Such an exemption, at least is such general character, is in our view neither appropriate nor justified. The EACB would therefore propose the deletion of Art 2(2)(b).

COM proposal	EACB proposal
(b) by the Union institutions, bodies, offices and agencies;	***~~(b) by the Union institutions, bodies, offices and agencies;~~***

[4] Towards a Coherent European Approach to Collective Redress, 15 July 2011, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-467.330%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

4.3. Data minimisation (Art 5(c))

The existing vertical legislation requires banks to collect a lot of personal data necessary to satisfy regulatory requirements and properly assess the individual circumstances and needs of their customers, such as for example in the context of the assessment of consumer's creditworthiness or assessment of the suitability of a given product. Under the Commission proposal for a Directive on credit relating to residential property (CARRP[5]) banks are under the obligation to *"obtain the necessary information regarding the consumer's personal and financial situation, his preferences and objectives".* Another example where banks are required to collect data is the AML Directive, which states that banks shall apply relevant customer due diligence measures which compromise identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source. The copy of or the references of the evidence required to perform the due diligence measures must be stored for at least five years after the business relationship with the bank's customer has ended.

The limitation, as proposed in the draft GDPR, 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 AML or creditworthiness assessment, or other. The EACB would therefore propose deletion of the reference to the 'minimum' and align the wording of Article 5(c) of the proposed regulation with the wording of Article 6(c) of the current Directive 95/46/EC on data protection.

COM proposal	EACB proposal
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 not involve personal data;***	Personal data must be: (...) (c) adequate, relevant, and ***not excessive*** ~~***limited to the minimum necessary***~~ in relation to the purposes for which they are ***collected and/or further*** processed; ~~***they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;***~~

4.4. Lawfulness of processing (Article 6 Paragraph 1)

The EACB would strongly recommend clarifying the provisions of Paragraph 1 point c of Article 6 of the proposal. According to this article, the processing of personal data is lawful if processing is necessary for compliance with a legal obligation to which the controller is subject. However, according to some national legislation personal data shall be processed only if the processing is based on the provisions of a legislative act or it is necessary for compliance with a task or obligation to which the controller is bound by virtue of a legislative act or an order issued on the basis of such an act. Therefore, the wording in the proposed regulation is more restrictive than the provisions of the existing national data protection laws.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0142:FIN:EN:PDF

In point f of Article 6 paragraph 1, the EACB would suggest widening up of the current wording to include orders, recommendations of competent organizations as well the requirements of supervisory authorities.

Finally, we suggest adding other particular cases of lawful processing of data.

COM proposal	EACB proposal
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 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.	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) the processing is based on the provisions of a legislative act or it is necessary for compliance with a task or obligation to which the controller is bound by virtue of a legislative act or an order issued on the basis of such an act;*** (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 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, ***or to processing carried out on the basis of orders, recommendations of competent organizations as well the requirements of supervisory authorities.*** ***(g)processing concerns data taken from public registers, lists, documents or records that are publicly available;*** ***(h) processing is carried out by non-profit associations, bodies or organisations, recognised or not, with regard either to entities having regular contacts with them or to their members, in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with the information notice provided for Article 14 Paragraph 2 of this Regulation.***

4.5. Conditions for consent (Art 7)

According to Article 7(4) of the proposed regulation, the consent shall not be a sufficient basis for data processing, if the data subject and the controller are in a "significant imbalance". In the context of the fact that the customer-bank relationship is generally perceived as asymmetrical, there is a risk that in practice the interpretation would be that consent could never lead to legitimising data processing by banks.

COM proposal	EACB proposal
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. ~~***4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.***~~

4.6. Processing of special categories of personal data (Article 9)

Under the national legislation of some Member States financial institutions can set up databases which contain data on fraud committed against the credit institutions. Processing and sharing of this data with other credit institutions is permitted in order to allow credit institutions to prevent fraud. Due to the restrictions envisaged in Article 9 of the proposal, i.e. processing of personal data concerning criminal convictions or related security measures, it is unclear whether such databases, the existence of which is essential to protect both consumers and businesses, can be maintained in the future. The EACB would strongly recommend clarifying that the restrictions envisaged in Article 9 Paragraph 1 are without prejudice to the operation of such databases.

In addition we notice that the processing of *health/medical related data* by specific sectors such as the banking and insurance sectors have not been taken into account. We 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. In fact, in the currently debated Proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation, in Article 2(7)[6] this

[6] Article 2(7) of the proposed Directive states: *"(...) in the provision of financial services Member States may permit proportionate differences in treatment where, for the product in question, the use of age or disability is a key factor in the assessment of risk based on relevant and accurate actuarial or statistical data"*. In the Council

specific role of health related factors is recognised. The EACB fears 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.

COM proposal	EACB proposal
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, 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. ***1a. (new) The prohibition as described in paragraph 1 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, as defined in Article 4(16) of this Regulation, and set up by financial institutions to prevent fraud.*** ***1b. (new) 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.***

4.7. Double regulation or conflicting regulation for banking industry (Art 22)

Under Article 22 of the Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions, banks are already under the obligation to have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and adequate internal control mechanisms, including sound administrative and accounting procedures. The organizational requirements for privacy management in enterprises in the proposed regulation on data protection (e.g. in Article 22) would generate overlaps with the existing obligations.

In addition, banks - in accordance with regulatory requirements in the field of fraud, money laundering and terrorist financing prevention - have had to commit to cover the processing of personal data. Therefore it is necessary to avoid regulatory duplication and contradictions. Once a bank fulfils its prudential obligations concerning corporate governance, those must be recognised in the context of data protection requirements. Moreover, possible conflicts between the Directive 2008/48/EC on consumer credit and Directive 2007/64/EC on payment services, and the new GDPR proposal should be carefully considered and eliminated.

compromise text of 19 October 2011, it is clearly stated that *"the use of age and disability in financial services, under clearly defined conditions, is not discrimination"*. Still, it is proposed to further enhance legal certainty in this respect, by removing the 'Member States option'.

COM proposal	EACB proposal
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) 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.***	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) 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 fulfillment of the requirements under Article 22 of the Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions shall be considered as fulfilling the requirements of this Article.*** ~~***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.***~~

4.8. Data protection officer (Articles 35-37)

Pursuant to Art 35 of the proposed regulation the designation of a Data Protection Officer is mandatory for enterprises employing 250 persons or more, or any company involved in processing operations which require regular and systemic monitoring of data subjects (by virtue of Article 35(1)(c)).

Article 28 of the proposed regulation introduces an obligation for controllers and processors to maintain documentation of the processing operations for which they are responsible which replaces the general obligation to notify individual processing operations to the supervisory authority, and makes the designation of a Data Protection Officer mandatory for enterprises employing 250 persons or more, or any company involved in processing operations which require regular and systemic monitoring of data

subjects. This requirement would mean that Data Protection officer would have to be designated by all banks.

It has to be considered that many companies (banks including) have implemented internal policies, directives and processes regarding the protection and the processing of personal data. Under Article 18 of the current Directive 95/46/EC, the controllers are under the obligation to notify the supervisory authority before carrying out any automatic processing operations. At the same time, Member States may provide for the simplification of or exemption from notification where the controller, in compliance with the national law, appoints a personal data protection official, thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations. Accordingly, as the principle the controllers were under the obligation to notify all data processing and as an exception they could appoint a data protection officer.

While it seems that the idea behind proposing the new solution in the new regulation was the willingness to reduce administrative burden of the controllers, the EACB considers that on the contrary the introduction of a duty to maintain detailed documentation of all processing operations is likely to create a considerable burden for the controllers who do not currently benefit from the option granted in Article 18 paragraph 2 of the Directive 95/46/EC. If undertakings have to both maintain documentation of the processing operations for which they are responsible and appoint a Data Protection Officer, the added value of a Data Protection Officer is absolutely not apparent. Thus, the EACB is strongly opposed to this change and would recommend deletion of Articles 35 - 37 of the proposed regulation[7].

COM proposal	EACB proposal
Article 35	~~***Article 35***~~
(…)	~~***(…)***~~
Article 36	~~***Article 36***~~
(…)	~~***(…)***~~
Article 37	~~***Article 37***~~
(…)	~~***(…)***~~

4.9. Transfer of Personal Data to Third Countries with an adequacy decisions (Art 41(2))

The earlier referred to Regulation 1781/2006 on information on the payer accompanying transfers of funds is also at stake in terms of third country transfers. Under Article 7 of the said Regulation, transfers of funds where the payment service provider (PSP) of the payee is situated outside of the EU, shall be accompanied by complete information about the payers, which under Art 4 of the same regulation shall consist of the payer's name, address (or alternatively the payer's date and place of birth, customer identification

[7] However, should the requirement for an obligatory designation of a Data Protection Officer be maintained, as a minimum the EACB would call to clarify that in case referred to in Paragraph 2 of the proposed Article 35, the obligation to appoint a single Data Protection Officer can also be fulfilled by a group of undertakings defined in Article 4(16) as amended by the EACB byoutsourcing relevant activities. This is particularly important for groups of small and local co-operative banks. We would therefore suggest the following wording of Paragraph 2 of Article 35:
*"2. In the case referred to in point (b) and (c) of paragraph 1**, a group of undertakings, as defined in Article 4 point 16 of this Regulation,** may appoint a single data protection officer **also by outsourcing the relevant activities."***

number or national identity number) and account number (or a unique identifier which allows the transaction to be traced back to the payer). In fact, the obligations under this regulation are about to be increased in terms of data to be transported.

On another point, the issue of the use of the standard contractual clauses for the transfer of personal data to processors established in non-EU countries that are not recognised as offering an adequate level of data protection, as last updated in February 2010, should be clarified in the new GDPR.

COM proposal	EACB proposal
1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation. (...) 5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).	1.A transfer may take place where ***it is required under the current EU legislation, including the Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds, or in other cases*** the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation. (...) 5. ***Without prejudice to the existing obligations of the payment service providers under Article 7 of the Regulation (EC) No 1781/2006, t***~~T~~he Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).

4.10. Transfers by way of binding corporate rules (Article 43)

The EACB in general agrees that binding corporate rules are important to improve the level of data protection. However, in our view the level of detail in the proposed Article 43 is too high We consider that the application of the consistency mechanism, with the timely involvement of the European Data Protection Board and the European Commission, would be a sufficient control mechanism and thus we would recommend a less prescriptive solution which would be more adjustable to the different circumstances on a case-by-case basis.

COM proposal	EACB proposal
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; (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;*** ***(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data;*** ***measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;*** ***(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;*** ***(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;*** ***(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;***	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; ***and*** (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;***~~ ~~***(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data;***~~ ~~***measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;***~~ ~~***(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;***~~ ~~***(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;***~~ ~~***(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;***~~

(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;	***~~(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;~~***
(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;	***~~(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;~~***
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;	***~~(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;~~***
(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.	***~~(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.~~***
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 binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.	***~~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 binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.~~***
4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	***~~4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).~~***

4.11. Courts competent to deal with complaints of data subjects (Art 75(2)

The EACB considers that the data subject should not be able to engage in proceedings against the controller in the Member State where the data subject is resident, and we would recommend to adhere to the spirit of the Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters ("Brussels I Regulation") by specifying that the proceedings shall be brought before the courts of the Member States where the processing of the data takes place.

COM proposal	EACB proposal
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or	2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or

processor has an establishment. ***Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.***	processor has an establishment ***or where the processing of the data takes place***. ~~***Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.***~~

4.12. Administrative sanctions (Art. 79)

As further explained in point 5 of this paper on *Delegated and implementing acts*, the EACB would strongly recommend investigating the compliance of paragraphs 3 – 7 of Article 79 with the Treaty on the European Union (TFEU) and the Treaty on the Functioning of the European Union (TFEU). Namely, regulation in the area of administrative proceedings and the imposition of administrative fines does not fall within the domain of the EU competence, and as such, under the principle so of subsidiarity it remains the sole responsibility of Member States. Thus, the first and foremost recommendation of the EACB would be a full deletion of paragraphs 3-7 of Article 79.

Should this Article be nevertheless maintained, we would like to point out that administrative sanctions should not be only based on the annual worldwide turnover of enterprises. This sole criterion can lead to a very disproportionate amount of fines and we consider that administrative sanctions should be limited to a fixed amount. Thus, we would insist, at the very least, on the following amendments.

COM proposal	EACB proposal
(…) 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: (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; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13; (c) does not comply with the right to be	(…) 4. The supervisory authority shall impose a fine up to ~~***250 000***~~ ***100 000 EUR***, or in case of an enterprise up to 0,5 % of its annual worldwide turnover ***and limited to a maximum of 100 000 EUR***, 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***~~ ***200 000 EUR***, or in case of an enterprise up to 1 % of its annual worldwide turnover ***and limited to a maximum of 200 000 EUR***, 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; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to

forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17; (d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18; (e) does not or not sufficiently determine the respective responsibilities with cocontrollers pursuant to Article 24; (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); (g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.	Article 13; (c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17; (d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18; (e) does not or not sufficiently determine the respective responsibilities with cocontrollers pursuant to Article 24; (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); (g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.
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:	6.The supervisory authority shall impose a fine up to ~~***1 000 000***~~ ***300 000 EUR*** or, in case of an enterprise up to 2 % of its annual worldwide turnover ***and limited to a maximum of 300 000 EUR***, to anyone who, intentionally or negligently:
(…) ***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.***~~

5. Delegated and implementing acts

The EACB is concerned about the extensive use of delegated and implementing acts in the proposed regulation. The regulation provides for the use of Commission delegated acts in no less than 26 different cases (which amounts to nearly a third of all provisions of the regulation). In addition, the Commission may adopt implementing acts for various purposes as outlined in Article 62.

In general, the EACB would like to warn that the extensive use of delegated acts renders the proposal akin to a framework directive whereby the provisions are likely to be subject to substantial change over time, as and when the Commission sees fit, and the EACB believes that this will result in a greater business and legal uncertainty for the industry. The EACB's concerns in this area can also be explained by the effective exclusion of stakeholders from the process of drawing up or preparing delegated acts which will create business uncertainty in the current time of continuing economic turmoil. Finally,

the EACB wishes to recall that according to Article 290 TFEU, delegated acts can only be applied to "non-essential" provisions of EU legislation, which could hardly be the case when a third of the proposed text is concerned.

The adoption of the implementing acts is to be done in accordance with the rules of the Regulation (EU) No 182/2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers. The EACB welcomes the choice made to apply the examination procedure which gives the committee composed of representatives of the Member States power to stop the Commission from adopting an implementing act concerning which the committee delivered a negative opinion. However, the EACB would recommend deletion of the possibility of applying Art 8 of the Regulation 182/2011 which allows the Commission in certain cases to adopt an immediately applicable implementing act without its prior submission to a committee. We therefore would call for deletion of Art 87(3) of the proposed data protection regulation.

In conclusion, the EACB objects such an extensive use of delegated acts, and strongly recommends significantly limiting the use of delegated acts in the new regulation. As the very least, the EACB would call for the following amendments:

- in Article 6(5): limiting the power of the Commission to adopt delegated act only to when the data subject is a child;
- In Article 12(5): deleting the Commission's power to issue delegated acts, as the Commission delegated acts should not, in our opinion, lead to further restrictions of the remedies of the processor against excessive and/or malicious requests;
- In Article 15(3): deleting the Commission's power to issue delegated acts;
- In Article 79(7): Deletion of Article 79(7); the EACB would strongly recommend investigating the compliance of paragraphs 3 – 7 of Article 79 with the Treaties on the European Union (TFEU) and on the Functioning of the European Union (TFEU). Namely, regulation in the area of administrative proceedings and the imposition of administrative fines does not fall under the domain of the EU competence, and as such, under the principle so of subsidiarity it remains the sole responsibility of Member States. Thus – at least – Art. 79(7) should be deleted.

COM proposal	EACB proposal
Article 6 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. _____ Article 12 ***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.*** _____ Article 15 ***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***	Article 6 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. _____ Article 12 ~~***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.***~~ _____ Article 15 ~~***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.	~~***the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.***~~
_____ Article 79 ***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.***	_____ Article 79 ~~***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.***~~

_____

Contact:

Marieke van Berkel, Head of Department
Tel: +32 2 286 98 47, Email: m.vanberkel@eurocoopbanks.coop

Katarzyna Kobylińska, Senior Adviser
Tel: +32 2 289 68 55, Email: k.kobylinska@eurocoopbanks.coop