



FEDERATION  
BANCAIRE  
FRANCAISE

**AMENDMENTS TO THE PROPOSAL FOR A REGULATION ON THE  
PROTECTION OF PERSONAL DATA**

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 4: Definitions</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>For the purposes of this Regulation:</p> <p>(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;</p> <p>(2) 'personal data' means any information relating to a data subject;</p> <p>(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;</p> <p>(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;</p> <p>(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law</p>	<p>For the purposes of this Regulation:</p> <p>(1) 'data subject' means an identified natural person or <b>a natural person</b> one who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;</p> <p>(2) 'personal data' means any information relating to a data subject;</p> <p>(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;</p> <p>(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;</p> <p>(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law</p>

or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(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;

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

(13) 'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the

or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed, **other than the controller, processor or data subject**;

(8) 'the data subject's consent' means any freely given specific, **and** 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;

(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

(13) 'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main

activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;

(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;

(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

(18) 'child' means any person below the age of 18 years;

(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.

processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;

(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;

(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings; **an undertaking controls one or more other undertakings if it exerts a dominant influence over that undertaking or those undertakings due to the direct or indirect holding of a fraction of the capital that confers on it the majority of voting rights at general meetings, or due to the rules that govern it or the power it has to enforce the rules on personal data protection.**

(17) 'binding corporate rules' means **a code of conduct defining the internal policy** on personal data protection, which is adhered to by a controller or processor established on the territory of a Member State of the Union, **for** transfers **or a set of** transfers of personal data **to** a controller or processor in one or more third countries within **an undertaking or a** group of undertakings;

(18) 'child' means any person below the age of 18 years;

(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46..

### ***Explanatory Memorandum***

A certain number of concepts used are subject to interpretation, because they do not correspond to any legal concepts shared on the European level (e.g. undertaking, group of undertakings, entities

(including natural persons)....).

Some formal amendments are made to the article to make the proposed text easier to understand.

Other adjustments are important:

- with regard to the definition of Consent, it is proposed that the term "explicit" be deleted, thereby returning to the definition of consent as set out in the 1995 directive.

When the lawfulness of processing is based on obtaining consent, the proposed regulation stipulates that the consent must be free, specific, informed and **explicit** (which requires a positive action on the part of the data subject). Yet this addition to the definition of consent is unrealistic and difficult to apply for all undertakings, which must preserve their freedom and the option of implementing innovative means in terms of the procedures for obtaining consent according to the vectors used (paper, internet, telephone) and the type of relationship initiated with the subjects.

- with regard to the definition of Undertaking in (15), it would be best to clarify that definition so that the branches that do not have a legal personality may be considered undertakings, within the regulation's meaning of data protection.

- with regard to the definition of Group of Undertakings in (16), it is proposed that the article be clarified by adding a paragraph to it to determine an objective control criterion that is easy to determine consisting of the reprise of recital 28 of the draft regulation: "

*A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.* »

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

### *Article 5: Principles relating to personal data processing*

Text proposed by the Commission	Proposed Amendment
<p>Personal data must be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;</p> <p>(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;</p> <p>(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;</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;</p> <p>(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.</p>	<p>Personal data must be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;</p> <p>(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;</p> <p>(c) adequate, relevant, and <b>not excessive limited to the minimum necessary</b> in relation to the purposes for which they are processed; <del>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;</del></p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified <b>without delay without unjustified delay</b>;</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;</p> <p>(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.</p>

### **Explanatory Memorandum**

The terms "limited to the minimum necessary" should be replaced by the words "not excessive," because these terms are in contradiction with Article 14.2 of the proposed regulation. Indeed, if only the "minimum" data are processed, the data supply cannot be optional.

The paragraph "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” is deleted, because it is no longer necessary since the concept of "not excessive data" is used. In addition, this paragraph is unnecessary, because the article covers personal data processing and the conditions for processing those data.

Finally, “without delay” is replaced by “without unjustified delay”: this satisfies practical considerations; data correction can take a certain amount of time to implement for technical reasons.

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 6</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p><i>Article 6</i> <b>Lawfulness of processing</b> 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. 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83. 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or</p>	<p><i>Article 6</i> <b>Lawfulness of processing</b> 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. 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83. 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or</p>



(b) the law of the Member State to which the controller is subject.  
 The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.  
 4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.  
 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

(b) the law of the Member State to which the controller is subject.  
 The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.  
 4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) (f) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.  
~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.~~

***Explanatory Memorandum***

Paragraph 4 does not refer to legitimate interest (6.1 f)) as a legal basis for subsequent processing when the purpose of that processing is incompatible with the purpose for which the data were collected: this article should be clarified to incorporate the exclusion of legitimate interest.

It has been requested that delegated act be deleted: The elements of the lawfulness of processing are essential with regard to the subject-matter of the regulation, and they cannot be taken by a delegated act (Article 290 of the Treaty).

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 7: Conditions for consent</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>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; <b>such proof may be based on the consent procedures established by the controller and/or the consent given by the data subject</b></p> <p>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.</p> <p>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.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject/<b>employee</b> and the controller/<b>employer</b>.</p> <p><b>5. The controller shall make a reasonable effort to obtain verifiable consent, given the technical means at his or her disposal.</b></p>
<b><i>Explanatory Memorandum</i></b>	
<p>This article raises the issue of the retention and traceability of the process of obtaining consent from the data subject; proof that consent was obtained by the data controller should be based on the procedures he or she has established for obtaining consent.</p> <p>It is essential that consent be easy to implement, specifically via the Internet, so that the processes are not made more labor-intensive.</p> <p>Moreover, the concepts of “employee” and “employer” are added to 7.4 to reflect the terms of recital 34.</p> <p>Finally, an 7.5 should be added: indeed, it is illogical that the technical limit set out in Article 7.1 should be reserved for children, but it should be applicable generally to the consent process.</p> <p>Note that this article creates a paradox: the data controller risks creating a specific file to index those persons who have given their consent and those who have not.</p>	

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

### Article 14 : Information to be provided **to** the data subject

Text proposed by the Commission	Proposed Amendment
<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;</p> <p>(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);</p> <p>(c) the period for which the personal data will be stored;</p> <p>(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;</p> <p>(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(f) the recipients or categories of recipients of the personal data;</p> <p>(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;</p> <p>(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.</p> <p>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.</p>	<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(a) the identity and the contact details of the controller <b>and, if any, of the controller's representative and of the data protection officer;</b></p> <p>(b) the purposes of the processing for which the personal data are intended, <b>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></p> <p><b>(c) the period for which the personal data will be stored;</b></p> <p>(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;</p> <p><b>(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</b></p> <p>(f) the recipients or categories of recipients of the personal data;</p> <p>(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;</p> <p><b>(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.</b></p> <p>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</p>

<p>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.</p> <p>4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:</p> <p>(a) at the time when the personal data are obtained from the data subject; or</p> <p>(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.</p> <p>5. Paragraphs 1 to 4 shall not apply, where:</p> <p>(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or</p> <p>(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</p> <p>(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or</p> <p>(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.</p> <p>6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.</p> <p>8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing</p>	<p>data.</p> <p>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.</p> <p>4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:</p> <p>(a) at the time when the personal data are obtained from the data subject; or</p> <p>(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.</p> <p>5. Paragraphs 1 to 4 shall not apply, where:</p> <p>(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or</p> <p>(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</p> <p>(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or</p> <p>(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.</p> <p>6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.</p> <p>8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and</p>
--	--

situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)

needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)

### ***Explanatory Memorandum***

A certain number of notices should be deleted, because they already appear in Article 15 when the subject exercises his or her right to access, or will be added to that article.

Much information is being added compared to what exists at present. From a technical viewpoint, this would result in increasing the size of the information notices that data controllers must enter on every contract, data collection form, including on web pages, when the current notices are already difficult to fit. Lengthening a notice is not necessarily an improvement for the subject-matters concerned.

In addition, with regard to the data protection officer, the data subject should contact the office in charge ("data protection officer for the undertaking"), not a natural person holding the position ("Mr./Ms. X"). A change in the person holding the position should not result in a systematic change in the contract documents that contain his or her name. This proposed amendment also has the benefit of ensuring better processing of requests issued by the data subjects.

The same is true for the data controller's representative.

In the event of any banking mediation in France, the contact details provided do not include the name of the natural person holding the position, and this system works fine.

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 15 : Right of access for the data subject</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>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:</p> <p>(a) the purposes of the processing;</p> <p>(b) the categories of personal data concerned;</p> <p>(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;</p> <p>(d) the period for which the personal data will be stored;</p> <p>(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;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any available information as to their source;</p> <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> <p>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</p>	<p>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:</p> <p>(a) the purposes of the processing); <b>and the legitimate interests pursued by the controller if the processing is based on Article 6, paragraph 1, point f);</b></p> <p>(b) the categories of personal data concerned;</p> <p>(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;</p> <p>(d) <b>the criteria for determining</b> the period for which the personal data will be stored;</p> <p>(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;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any available information as to their source;</p> <p><del>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20;</del></p> <p><b>i) where applicable, the contact details of the controller's representative and that of the data protection officer</b></p>

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 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).

**j) any other information that is required to ensure faithful data processing with regard to the data subject, given the particular circumstances in which the personal data are collected.**

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 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).

### ***Explanatory Memorandum***

Proposal to add certain fields to Article 15 that were initially in Article 14. With regard to the storage period, it is proposed that only those criteria that are used to determine the data storage period be disclosed to the data subjects (15.1.d)).

Need to specify what “significance and envisaged consequences” (1.h) means. Otherwise, it is proposed that h) be deleted so as not to cause the data subject any needless worry. The subject is already aware of the purposes of the processing.

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

### **Article 31.1: Notification of a personal data breach to the supervisory authority**

<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.	1. In the case of a personal data breach, the controller shall, <del>without undue delay and, where feasible, not later than 24 hours</del> <b>within a reasonable time</b> after having become aware of it, notify the personal data breach to the supervisory authority. <del>The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</del>

### ***Explanatory Memorandum***

The words “without undue delay and, where feasible, not later than 24 hours” should be replaced by “within a reasonable time,” because a security breach requires investigations to find out the exact causes and consequences for data protection. These investigations may take some time, given the complexity of the information systems and the various possible sources of the breaches (human error, technical issues, tampering, etc.). Evaluating the scope of subjects who may be affected also takes time.

Delete the last sentence in 1, which no longer has any purpose if the 24-hour concept is deleted.



# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 31.6 : <i>Notification of a personal data breach to the supervisory authority</i></b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>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).</p>	<p><del>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).</del></p>
<p style="text-align: center;"><b><i>Explanatory Memorandum</i></b></p> <p>Applicable procedures and the way the documents are compiled should be left to the discretion of each institution. That being the case, this subparagraph should be deleted.</p>	

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 32.1 : <i>Communication of a personal data breach to the data subject</i></b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p>	<p>1. When the personal data breach <del>is likely to adversely affect</del>s the <del>protection of the personal data or</del> privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p>
<p style="text-align: center;"><b><i>Explanatory Memorandum</i></b></p> <p>Delete "is likely," because only those breaches that have established consequences should be communicated to the data subject. Delete the idea of adversely affecting the protection of the data, which is too broad, because by definition this means all breaches.</p>	

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

### **Article 32.5: *Communication of a personal data breach to the data subject***

<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p>	<p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach <del>is likely to</del> adversely affects <b>the private life of the data subject.</b> personal data referred to in paragraph 1.</p>
<p style="text-align: center;"><b><i>Explanatory Memorandum</i></b></p> <p>(See similar amendment in 1. of the same article).</p>	

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 33.2: Data protection impact assessment</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p><i>Article 33</i>  <b>Data protection impact assessment</b>            1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.            2. The following processing operations in particular present specific risks referred to in paragraph 1:</p>	<p><i>Article 33</i>  <b>Data protection impact assessment</b>            1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.            2. The following processing operations <del>in particular</del> present specific risks referred to in paragraph 1:</p>
<p><b>Explanatory Memorandum</b></p> <p>The obligation to perform an impact study can be sanctioned by a fine of €1,000,000 or 2% of annual worldwide turnover for an undertaking, and because the concept of "specific risks" is vague and open to interpretation, this obligation should be limited to the processing transactions listed in Article 33 by deleting the term "in particular," which will ensure better legal security.</p>	

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

### **Article 33 .2 c): *Data protection impact assessment***

<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p>	<p>Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations <del>in particular</del> present specific risks referred to in paragraph 1:</p> <p>c) monitoring publicly accessible areas, <b>except for banking devices</b>, especially when using optic-electronic devices (video surveillance) on a large scale;</p>

### ***Explanatory Memorandum***

Certain activities, such as banking activity, require the use of opto-electronic devices (video surveillance) to guarantee the security of employees, clients, and the public. As such, and given the need to use these devices, the obligation to run an impact study should be removed for these activities, especially since it would be impossible for the data controller to obtain the consent of the data subjects as set out in 33.4.

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 33.4: Data protection impact assessment</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations</p>	<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>4. <del>The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</del></p>
<p style="text-align: center;"><b>Explanatory Memorandum</b></p> <p>Systematically obtaining the consent of data subjects for all processing that undergoes impact assessment is impossible or would lead to deploying efforts or incurring costs that are out of proportion, especially for large-scale processing. For these reasons, paragraph 4 of article 33 should be deleted.</p>	

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

### **Article 33.6: *Data protection impact assessment***

<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p>	<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>6. <del>The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</del></p>

### ***Explanatory Memorandum***

The criteria and conditions applicable to processing that are likely to present particular risks, the content of the impact assessment, and the conditions of modularity, verification and auditability are essential elements that should appear in the regulation itself. As a result, paragraph 6, which refers the task of providing details on the aforementioned points to delegated acts, should be deleted.

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

### Article 35.2: *Designation of the data protection officer*

Text proposed by the Commission	Proposed Amendment
<p>1. The controller and the processor shall designate a data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p>	<p>1. The controller and the processor shall designate a data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p><b>The group of undertakings may also appoint a single data protection officer for one or more processing operations implemented by several of the group's entities.</b></p>

#### ***Explanatory Memorandum***

In groups of undertakings, only certain processing operations can be common to different undertakings for cross-cutting disciplines (human resources, anti-money laundering, anti-terrorist financing, etc.), without the other processing operations being shared.

Therefore, the option should be considered for the group to appoint a single data protection officer solely for those processing operations that are implemented by several of the group's entities.

Consequently, a second subparagraph should be added to Article 35 2): **“The group of undertakings may also appoint a single data protection officer for one or more processing operations implemented by several of the group’s entities.”**



# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 35.7) : Designation of the data protection officer</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p>	<p>7. The controller or the processor shall designate a data protection officer associated with a <b>sufficient hierarchical level</b> and for a period of at least two years. The data protection officer may be reappointed for further terms. <del>During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</del></p>
<p style="text-align: center;"><b>Explanatory Memorandum</b></p> <p>Creating a specific status of data protection officer would be a source of constraints and difficulties.</p> <p>Conversely, to ensure his or her independence, association with a hierarchical level should be provided, as is the case under French law for the person responsible for compliance.</p>	

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

### **Article 35. 9) and 10): *Designation of the data protection officer***

<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.</p> <p>10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p>	<p>9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority <b>and to the public</b>.</p> <p>10. Data subjects shall have the right to contact <b>the office designated by</b> the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p>
<p style="text-align: center;"><b><i>Explanatory Memorandum</i></b></p> <p>It is proposed that the option of communicating the officer's contact details <b>to the public</b> be deleted, because this could cause too great a disturbance for the officer. Subjects should be able, as they currently are, to contact the data controller, who will decide whether or not the matter should be referred to the officer.</p> <p>Undertakings must retain the option of determining the organization they want to establish so that subjects whose data are processed may effectively exercise their rights. Therefore, we propose that the requests may be sent to the office designated by the officer. Consequently, "<b>the office designated by</b>" should be added after the "<b>the right to contact.</b>" In addition, the data protection officer cannot be the sole point of entry for all requests, which might contaminate his activity.</p>	

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 37: Tasks of the data protection officer</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>1. The controller or the processor shall entrust the data protection officer at least with the following tasks:</p> <p>(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;</p> <p>(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</p> <p>(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;</p> <p>(d) to ensure that the documentation referred to in Article 28 is maintained;</p> <p>(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;</p> <p>(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior</p>	<p>1. The controller or the processor shall entrust the data protection officer at least with the following tasks:</p> <p>(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;</p> <p>(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</p> <p>(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;</p> <p>(d) to ensure that the documentation referred to in Article 28 is maintained;</p> <p>(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;</p> <p>(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33</p>

<p>consultation, if required pursuant Articles 33 and 34;</p> <p>(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;</p> <p>(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.</p> <p>2.</p>	<p>and 34;</p> <p>(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;</p> <p>(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.</p> <p><b>2. In the performance of the tasks set out in paragraph 1, officers from supervised regulated financial professions may call on the audit services of the data protection officer.</b></p>
--	--

***Explanatory Memorandum***

Point 2: For credit institutions, banking regulations already provide audit and internal control procedures. In the aim of effectiveness, and to avoid duplicating existing organizations that have already been tested, the data protection officer might be allowed to use existing audit services in the course of his or her duties.

Consequently, we propose inserting a point 2 specific to the regulated financial professions that are supervised: "In the performance of the tasks set out in paragraph 1, officers from regulated financial professions monitored by an overseer may call on the audit services of the data protection officer."

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

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

### ***Explanatory Memorandum***

Paragraphs 2 and 3 introduce the concept of class actions. A regulation on data protection cannot be the legal basis for class actions, which are furthermore reviewed with regard to the different domestic laws and in the context of the Commission's specific work.

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 76 – 1</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>Article 76</p> <p><i>Article 76</i> <b>Common rules for court proceedings</b> 1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.</p>	<p><i>Article 76</i> <b>Common rules for court proceedings</b> <del>1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.</del></p>
<p style="text-align: center;"><b><i>Explanatory Memorandum</i></b></p> <p>Paragraph 1 makes reference to Article 73 – 2, which introduced the concept of class actions. In the interest of consistency, this paragraph should be deleted, because a regulation on data protection cannot be the legal basis for class actions.</p>	

# FEDERATION BANCAIRE FRANCAISE

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 79 Administrative sanctions</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p><i>Article 79</i> <b>Administrative sanctions</b></p> <p>1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.</p> <p>2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.</p> <p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p> <p>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</p>	<p><i>Article 79</i> <b>Administrative sanctions</b></p> <p>1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.</p> <p>2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.</p> <p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p> <p>4. The supervisory authority shall impose a fine up to 250 000 EUR, <b>or in case of an enterprise up to 0,5 % of its annual</b></p>



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 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

~~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 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:

- (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;
- (b) processes special categories of data in violation of Articles 9 and 81;
- (c) does not comply with an objection or the requirement pursuant to Article 19;
- (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;
- (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;
- (f) does not designate a representative pursuant to Article 25;
- (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;
- (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;
- (i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;
- (j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;
- (k) misuses a data protection seal or mark in the meaning of Article 39;
- (l) carries out or instructs a data transfer to a

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:

- (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;
- (b) processes special categories of data in violation of Articles 9 and 81;
- (c) does not comply with an objection or the requirement pursuant to Article 19;
- (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;
- (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;
- (f) does not designate a representative pursuant to Article 25;
- (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;
- (h) does not alert on or notify a personal data breach ~~or does not timely or completely notify the data breach~~ to the supervisory authority or to the data subject pursuant to Articles 31 and 32;
- (i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;
- (j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;
- (k) misuses a data protection seal or mark in the meaning of Article 39;
- (l) carries out or instructs a data transfer to a

<p>third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;</p> <p>(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);</p> <p>(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);</p> <p>(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.</p> <p>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.</p>	<p>third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;</p> <p>(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);</p> <p>(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);</p> <p>(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.</p> <p><del>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.</del></p>
--	---

***Explanatory Memorandum***

Administrative sanctions should not be based on the annual worldwide turnover of enterprises. This criterion would result in penalty amounts that are out of all proportion with the breaches and their impact on the data subjects. These criteria that exist with regard to competition law are not justified in matters of data protection, where there is no damage to the market, but to the private interests that are individual rights. Compensation for any damages suffered may be made before the civil courts by means of an action for damages.

# FRENCH BANKING FEDERATION

## PROPOSAL FOR A REGULATION ON PERSONAL DATA PROTECTION

<b>Article 86 – 2°</b>	
<b>Text proposed by the Commission</b>	<b>Proposed Amendment</b>
<p>Article 86 - 2°</p> <p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p>	<p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for <b>an indeterminate a period of two years</b> <del>time</del> <b>from the publication date of entry into force of this Regulation.</b></p>
<b><i>Explanatory Memorandum</i></b>	
<p>In the interest of legal security and consistency between the regulation's publication date and its deadline for entry into force, it is important that the Commission take all of the required delegated acts before the regulation comes into force.</p>	