European Banking Federation

GENERAL DATA PROTECTION REGULATION: EUROPEAN BANKING FEDERATION SUGGESTIONS FOR AMENDMENT TO THE CHAPTER IV *(on the basis of the Council text – version of 17 September 2014)*

I. EBF key priorities regarding Chapter IV

A. Data breach notification – Articles 31 &32

- The notification requirement should be limited to serious breaches affecting a significant number of individual data subjects, based on a thorough assessment. To ensure legal certainty, there should be consistency between the definitions proposed in the General Data Protection Regulation and the Network and Information security Directive.
- An exemption should be awarded where encryption or other appropriate security measures are used or if the controller takes appropriate measures to adequately compensate those affected. In this regard EBF welcomes Article 32.2 a) b) and c).
- Organisations should be able to have some flexibility regarding decisions and delays of communication of personal data breach to data subjects to facilitate appropriate investigation and other measures to understand the scope scale and potential impact of a data breach, if any.

B. impact assessment – Article 33

- A new privacy impact assessment should be required only where a process or project poses substantially new or different privacy risks from what has been analysed in the past and a single impact assessment shall be sufficient to address a set of similar operations that present similar risks. In addition, it would seem disproportionate to impose an overall obligation on controllers to seek the views of data subjects, whatever the sector, before any data processing had been done.

C. Data protection officer – Article 35

- According to a risk-based model, data controllers should only be obliged to have data protection officers if personal data processing is a substantial part of the business operations. However, the appointment of a DPO should consequently lead to exoneration of administrative burdens, such as obligation to process.

European Banking Federation

II. Specific amendments on Chapter IV

- **Joint controllers**

EBF Amendment n°	Article	Text proposed by the Council of the EU *(version of 17 September 2014)*	Amendment proposed
1.	**Article 24**	1. Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement should designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.	1. Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner determine their respective responsibilities, for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. **The arrangement shall duly reflect the joint controllers' respective effective roles, relationships and responsibilities vis-à-vis data subjects.**
		2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in	2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the (…) controllers unless the data

		respect of and against each of the (...) controllers unless the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible. The data subject may nevertheless exercise his or her rights under this Regulation in respect of and against each of the controllers if the arrangement is unfairly detrimental to his or her rights and interests.	subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible. The data subject may nevertheless exercise his or her rights under this Regulation in respect of and against each of the controllers if the arrangement is unfairly detrimental to his or her rights and interests.
Justification			
The arrangement to be entered into by joint controllers should be expressly required to duly reflect the joint controllers' respective roles and relationships with the data subjects.			

- **Security of processing**

EBF Amendment n°	**Article**	**Text proposed by the Council of the EU** ***(version of 17 September 2014)***	**Amendment proposed**
2.	**Article 30**	1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing as well as the likelihood and severity of the risks for the rights and freedoms of data subjects, the controller and the processor shall implement appropriate technical and organisational measures, including encryption, anonymisation and pseudonymisation of personal data to ensure a level of security appropriate to these risks.	1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing as well as the likelihood and severity of the risks for the rights and freedoms of data subjects, the controller and the processor shall implement appropriate technical and organisational measures, ~~**including**~~ **such as** encryption, anonymisation and pseudonymisation of personal data to ensure a level of security appropriate to these risks.

		1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing (…), in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 2. (…) 2a. The controller and processor may demonstrate compliance with the requirements set out in paragraph 1 by means of adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39. 2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. 3. (…) 4. (…)	1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing (…), in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 2. (…) 2a. The controller and processor may demonstrate compliance with the requirements set out in paragraph 1 by means of adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39. 2b. The controller and processor shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. 3. (…) 4. (…)
Justification			
Technical and organisational measures for security processing should not only be limited to encryption, anonymisation and pseudonymisation of personal data as other technics should be developed in the future. Therefore those measures should be presented as examples.			

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

European Banking Federation

EBF Amendment n°	Article	Text proposed by the Council of the EU *(version of 17 September 2014)*	Amendment proposed
3.	**Article 31**	1. In the case of a personal data breach which is likely to result in a specific risk for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, breach of anonymity or pseudonymity, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.	1. In the case of ~~a~~ **any significantly harmful** personal data breach which is likely to result in a specific risk for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, breach of anonymity or pseudonymity, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay ~~**and, where feasible, not later than 72 hours after having become aware of it**~~, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification **without undue delay** ~~**in cases where it is not made within 72 hours**~~. **A significantly harmful personal data breach shall be determined by the controller, who can be assisted by the data protection officer, based on factors including the assessment of whether a personal data breach has created serious breaches for a significant number of data subjects.** **Exemptions from data breach provisions should be awarded where encryption or other appropriate data security measures are used or if measures are taken to adequately compensate or assist those affected.**

		1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b). 2. (…) The processor shall notify the controller without undue delay after becoming aware 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, where possible and appropriate, the approximate categories and number of data subjects concerned and the categories and approximate 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) (…) (d) describe the likely consequences of the personal data breach identified by the controller; (e) describe the measures taken or proposed to be taken by the controller to address the personal data breach; and (f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach. 3a. Where, and in so far as, it is not possible to	1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b). 2. (…) The processor shall notify the controller without undue delay after becoming aware 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, where possible and appropriate, the approximate categories and number of data subjects concerned and the categories and approximate 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) (…) (d) describe the likely consequences of the personal data breach identified by the controller; (e) describe the measures taken or proposed to be taken by the controller to address the personal data breach; and (f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.

European Banking Federation

		provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay. 4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, 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. (…). 5. Pursuant to Union law or the law of a Member State the competent supervisory authority shall inform the national information security authorities without undue delay about the 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).	3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay. 4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, 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. (…). 5. Pursuant to Union law or the law of a Member State the competent supervisory authority shall inform the national information security authorities without undue delay about the data breach. ~~**6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**~~
Justification			

- **Introducing an obligation to notify personal data breaches in 24 hours, as stated in the European Commission proposal, for other sectors than the telecommunications sectors appears disproportionate and practically impossible to implement. We are therefore more in favour of the Presidency of the EU proposing "*without undue delay and where feasible*".**

  A framework where notification is made in the most expedient time possible would achieve the goal of ensuring regulators and data subjects are well informed without causing unnecessary burden for regulators or alarm to victims of breaches.

- Attention should be paid to the criteria which trigger the obligation to notify: **the notification requirement should be limited to serious breaches affecting significant number of individuals.** Otherwise, there is a danger of triggering an avalanche of notifications with the potential to confuse or unnecessarily alarm individuals or desensitise affected data subjects. Financial institutions fully understand that there are circumstances that require notification to a financial and or data protection regulator in the event of a breach. **However, this obligation could create duplicative reporting obligation and might even conflict with national financial law and regulation.**
  To ensure legal certainty, the definitions within the General Data Protection Regulation and the Network and Information security Directive should be consistent.

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

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

- It is unlikely that delegated acts will be adopted at the moment when the Regulation will start to apply. Therefore the new obligations cannot effectively be implemented in the sense that, if no delegated act is in place, every single data breach will have to be notified to the national supervisory authority.
  In the absence of clear provisions ensuring legal certainty, the national supervisory authorities' practices might be highly inconsistent.

  Therefore, we are of the view that the rules regarding data breach notifications constitute essential elements of the proposal within the meaning of Article 290 of the Treaty on the Functioning of the European Union (TFEU) (Opinion shared by the EDPS and the Working Party Article 29) and should not be left to be regulated by means of delegated acts.

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

European Banking Federation

EBF Amendment n°	Article	Text proposed by the Council of the EU *(version of 17 September 2014)*	Amendment proposed
4.	**Article 32**	1. When the personal data breach is likely to result in a specific risk for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, damage of reputation, breach of anonymity or pseudonymity, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall (...) communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the	1. **In the case of any significantly harmful personal data breach,** when the personal data breach is likely to result in a specific risk for the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, damage of reputation, breach of anonymity or pseudonymity, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. **A significantly harmful personal data breach shall be determined by the controller based on factors including the assessment of whether a personal data breach has created serious breaches for data subjects.** **Exemptions from data breach provisions should be awarded where encryption or other appropriate data security measures a used or if measures are taken to adequately compensate or assist those affected.** 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for

		personal data breach and contain at least the information and the recommendations provided for in points (b), (e) and (f) of Article 31(3). **III.** The communication (…) to the data subject referred to in paragraph 1 shall not be required if: a. the controller (…) has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or b. the controller has taken subsequent measures which ensure that the specific risks for the rights and freedoms of data subjects referred to in paragraph 1 are no longer likely to materialise; or c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or d. it would adversely affect a substantial public interest . 4. (…) 5. (…) 6. (...)	in points (b) and (c) of Article 31(3). 3. The communication (…) to the data subject referred to in paragraph 1 shall not be required if: a. the controller (…) has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or b. the controller has taken subsequent measures which ensure that the specific risks for the rights and freedoms of data subjects referred to in paragraph 1 are no longer likely to materialise; or c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or d. it would adversely affect a substantial public interest . 4. (…) 5. (…) 6. (...)
Justification			
• Attention should be paid to the criteria which trigger the obligation to communicate. There is a danger of triggering an avalanche of			

notifications with the potential to confuse unnecessary alarm individuals or desensitise affected data subject. Moreover, a communication to the public could result in an invitation for criminals to take advantage of the situation (e.g. phishing, or attacking the system from which the data leaked in first place).

At present, banks already notify their customers for instance if their credit card has been skimmed (i.e. information about a card and the associated PIN-code is copied for the purpose of manufacturing a fake card). It is also in the bank's interest to protect their customers against fraud and sustain a very high level of security. The banks can also be held liable for damages their customers may suffer due to deficiencies in banks IT- security systems. The banks test and update their systems and security solutions regularly to make sure that the information in the bank's system is always well-protected and secure. The transfer of information between the customer´s computer and the online banking system is always encrypted. The customer must also make sure that his/her computer, codes and personal information are protected to prevent the possibility of fraud. To avoid "data breaches" it would be more effective to inform customers on how to protect their own computers, never disclose their bank account details to unknown persons etc.

- **We believe that an exemption should be awarded where sophisticated encryption or other appropriate data security measures are used or if measures are taken to adequately compensate or assist those affected. We therefore welcomes the provisions in Article 32.3a): technological protection/encryption), 32.3b): subsequent measures and 32.3c): information of the data subject owing to the number of cases involved.**
- **Organisations should be able to have some flexibility regarding decisions and delays of communication of personal data breach to data subjects.** Indeed, strict and mandatory information requirements even in some minor cases would impose significant compliance burdens to controllers. Moreover, such notifications to the public can potentially compromise the security of such organisations and result in financial crime and/or more breaches.
- A framework where notification is made in the most expedient time possible would achieve the goal of ensuring that regulators and data subjects are well-informed without causing an unnecessary burden for regulators or alarm to potential victims of breaches. **The EBF therefore welcome the reference to "*without undue delay*".**

- **Data protection impact assessment**

EBF Amendment	Article	Text proposed by the Council of the EU *(version*	Amendment proposed

European Banking Federation

n°		*of 17 September 2014)*	
5.	**Article 33**	1. Where the processing, taking into account the nature, scope context, or purposes of the processing, is likely to result in a specific risk for the rights and freedoms of data subjects , such as discrimination, identity theft or fraud, financial loss, damage of reputation, breach of anonymity or pseudonymity , loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage , the controller (…) shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…) .	1. Where the processing, taking into account the nature, scope context, or purposes of the processing, is likely to result in a specific risk for the rights and freedoms of data subjects , such as discrimination, identity theft or fraud, financial loss, damage of reputation, breach of anonymity or pseudonymity , loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage , the controller (…) shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…) . **A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.**
		1a. The controller shall seek the advice of the data protection officer, where applicable, when carrying a data protection impact assessment.	1a. The controller shall seek the advice of the data protection officer, where applicable, when carrying a data protection impact assessment.
		2. A data protection impact assessment referred to in paragraph 1 shall be required in the following cases:	2. A data protection impact assessment referred to in paragraph 1 shall be required in the following cases:
		(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions are based that produce legal effects concerning data subjects or severely affect data	~~[(a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions are based that produce legal effects concerning data subjects or severely affect data subjects;]~~

		subjects; (b) processing of special categories of personal data under Article 9(1) (...) , biometric data or data on criminal convictions and offences or related security measures, where the data are processed for taking (...) decisions regarding specific individuals on a large scale ; (c) monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices (...) ; (d) (...); (dd) processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where reasonable expectations are not met, for example owing to the context of the processing operation; (de) processing operations involving personal data which have especially far-reaching consequences, which are in particular irreversible or discriminatory, which prevent data subjects from exercising a right or using a service or a contract, or which have a major impact on a large number of persons; (e) other operations where the competent supervisory authority considers that the processing is likely to result in a specific risk for the rights and	(b) processing of special categories of personal data under Article 9(1) (...) , biometric data or data on criminal convictions and offences or related security measures, where the data are processed for taking (...) decisions regarding specific individuals on a large scale ; (c) monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices (...); (d) personal data in large scale processing systems containing genetic data or biometric data; dd) processing operations involving personal data which are particularly invasive, for example, on account of their secrecy, where a new technology is used, where it is more difficult for data subjects to exercise their rights, or where reasonable expectations are not met, for example owing to the context of the processing operation; (de) processing operations involving personal data which have especially far-reaching consequences, which are in particular irreversible or discriminatory, which prevent data subjects from exercising a right or using a service or a contract, or which have a major impact on a large number of persons; (e) other operations where the competent supervisory authority considers that the processing is likely to result in a specific risk for the rights and freedoms of data subjects, in particular because

		freedoms of data subjects, in particular because they render the exercise by data subjects of their rights under this Regulation more difficult	they render the exercise by data subjects of their rights under this Regulation more difficult.
		2a. The supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.	2a. The supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.
		2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.	2b. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.
		2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.	2c. Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
		3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risks referred to in paragraph 1, the measures envisaged to	3. The assessment shall contain at least a general description of the envisaged processing operations, an evaluation of the risks referred to in paragraph 1, the measures envisaged to address the risks including safeguards, security

		address the risks including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned . 3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. 4. The controller shall carry out the assessment at the request of the data subjects without prejudice to the protection of commercial or public interests or the security of the processing operations and make it available in an appropriate form . 5. (...) Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question , paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities. 6. (...)	measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned . 3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. 4. ~~**The controller shall carry out the assessment at the request of the data subjects without prejudice to the protection of commercial or public interests or the security of the processing operations and make it available in an appropriate form.**~~ 5. (...) Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question , paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities..

		7. (…)	6. (…) 7. (…)

Justification

- A new privacy impact assessment should be required only where a process or project poses substantially new or different privacy risks from what has been analysed in the past. In addition, it would seem disproportionate to impose an overall obligation on controllers to seek the views of data subjects, whatever the sector, before any data processing had been done. In this sense, we very much welcome the amendments to Article 33(1) and Article 33(4) in the LIBE committee text.

- **Designation of the data protection officer**

EBF Amendment n°	Article	Text proposed by the Council of the EU *(version of 17 September 2014)*	Amendment proposed
6.	**Article 35**	1. The controller or the processor may, **or where required by Union or Member State law shall**, designate a data protection officer (…). 2. A group of undertakings may appoint a single data protection officer. 3. Where the controller or the processor is a public authority or body, a single data protection	1. The controller or the processor may, ~~**or where required by Union or Member State law shall**~~, designate a data protection officer (…). 2. A group of undertakings may appoint a single data protection officer. 3. Where the controller or the processor is a public authority or body, a single data protection officer

		officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.	may be designated for several such authorities or bodies, taking account of their organisational structure and size.
		4. (…).	4. (…).
		5. The (…) data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37, particularly the absence of any conflict of interests (…).	5. The (…) data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37, particularly the absence of any conflict of interests (…).
		6. (…)	6. (…)
		7. (…). During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her tasks pursuant to Article 37.	7. (…). During their term of office, the data protection officer **shall have a level of management autonomy and** may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her tasks pursuant to Article 37.
		8. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.	8. The data protection officer **of the controller or of the processor** may be**, according to their sole decision**, a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
		9. The controller or the processor shall publish the contact details of the data protection officer and communicate these to the supervisory authority (…).	9. The controller or the processor shall ~~**publish**~~ **communicate** the contact details of the data protection officer to the supervisory authority

European Banking Federation

		10. Data subjects may contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation. 11. (...)	(...). 10. Data subjects may contact the data protection officer or **any delegated officer** on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation. 11. (...)
Justification Moreover, the appointment of a new significantly important position of the DPO in the organization as bank which process a substantial amount of personal data shall be governed by the internal rules of the organization. Thus, the controller and the processor shall have autonomy on deciding whether to appoint the DPO as an employee or as an independent service provider. In the EBF views, to ensure the independence of the DPO, it has to have a functional independence. The EBF believes that the contact details of the DPO should not be communicated to the public (otherwise personal data of a DPO will not be protected the same way as the data of other employees). Indeed, we note that the public can contact the controller who will decide whether or not it is necessary to contact or not the DPO.			