

Eurofinas observations and proposal for amendments on the ITRE draft opinion on the Proposal for a General Data Protection Regulation

Eurofinas, the voice of consumer credit providers at European level, believes that the Commission Proposal for a General Data Protection Regulation provides a good starting point to further discussions and debate on the EU framework for the protection of personal data. We have taken note of the draft opinion of the Industry, Research and Energy Committee and would like to share our views on this document with you. The below should be read in light of the Eurofinas observations on the Proposal.¹

The draft ITRE opinion on this Proposal addresses the concerns of the industry in a number of areas. **In particular we support the following amendments incorporated in the draft opinion:**

- **Amendment 6 and 30: Recital 38, Article 6(1)(f) – Legitimate interests**
These amendments ensures that data can be processed for the legitimate interests pursued by the controller and the third party/parties to whom the data are communicated, in line with the currently applicable Directive 95/46/EC
- **Amendment 34: Article 7(1) - Consent**
There is no justification for a burden of proof for the controller only, especially in cases where the data subject has the consent in his personal documents. We support the deletion of this provision.
- **Amendment 29: Article 6(1)(a) – Specific purposes**
In some Member States, consumers give consent for the processing of their data for general purposes. If consent were to be required for each separate purpose, this would be disproportionately time-consuming, resource-intensive and costly.
- **Amendment 47, 48, 49, 50, 56: Article 14(1)(b), Article 14(1)(c), Article 14(1)(e), Article 14(1)(h), Article 15(1)(f) – Information to be provided to data subjects**
We support the amendments put forward in this area. Data subjects will already have been provided the contract terms and conditions when they signed this contract and there is no reason for duplications. Periods for data storage are often not known at the time the data is collected, especially in highly regulated sectors such as financial services where anti-money laundering requires the collection and storage of data throughout the relationship with the client, which may be of an indeterminate period of time.
- **Amendment 52: Article 14(3) – Publicly available data**
As the data is already publicly available, such a warranty is not necessary to ensure the protection of fundamental rights. The data has already been published and the data subject already knows this and that his or her data may be processed by third parties.

¹ See <http://www.eurofinas.org/uploads/documents/positions/Eurofinas%20observations%20-%20final.pdf>.

- **Amendment 62: Article 17(3)(d) – Erasure**
The amendment would increase legal certainty for controllers who are obliged to process data in accordance with legal obligations.
- **Amendment 93: Article 33(4) – Impact Assessments**
We support deletion of this provision as it will be impossible to implement in practice for controllers to seek the views of data subjects’ representatives and they may not always have the expertise, qualifications or resources to respond to such imposed requests for their views;
- **Amendment 125 - 153: Article 79(3) – Article 79(7) – Sanctions**
Supervisory authorities should not be obliged to impose sanctions, they should only impose sanctions after taking into account all circumstances of each individual case.
- **Amendments 20, 33, 40, 45, 46, 57, 64, 73, 77, 79, 80 85, 87, 89, 91, 9, 114, 156, 157: Recital 129, Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 15(3), Article 17(9), Article 20(5), Article 22(4), Article 23(3), Article 23(4), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 34(8), Article 44(7), Article 81(3), Article 82(3) – Delegated and implementing acts**
Delegated and implementing acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty, we therefore fully support a reduction in the number of delegated acts.
- **Amendment 28, 44, 71 and 158: Article 4(19a) (new), Article 9(2)(j), Article 20(2)(cb) (new) and Article 83 (a) (new) – Processing of criminal convictions data for the purpose of the prevention of financial crime**
We support these provisions, as it enables financial institutions to detect and prevent fraud. However, this is only one of many measures that we feel should be taken in this area.

Therefore, in addition, we would also like to suggest a number of further amendments:

Amendment 1 – Data minimisation
Article 5(c)

Original wording	Proposed amendment
Personal data must be: (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;	Personal data must be: (c) adequate, relevant, and not excessive 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;

Justification

The obligation to process the minimum data necessary would contradict with legal provisions which require, e.g. lending institutions, to process personal data such as the Consumer Credit Directive and the Capital Requirements Package. Therefore wording of Directive 95/46/EC which permits “not excessive” processing is more appropriate.

Amendment 2 – Lawfulness of processing

Article 6(1)(c)

Original wording	Proposed amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(c) processing is necessary for compliance with a legal obligation, regulatory rule, guidance, industry code of practice, either domestically or internationally to which the controller is subject including the requirements of supervisory authorities;</p>

Justification

Article 6(1)(c) should be widened-up to ensure that domestic financial regulation or codes of conduct are included, in particular the requirements of supervisory authorities.

Amendment 3 – Legitimate interest

Article 6(1)(f)

Original wording	Proposed amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(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.</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. It is within the controller's legitimate interests to prevent and detect fraud.</p> <p>OR</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to</p>

	<p>processing carried out by public authorities in the performance of their tasks.</p> <p><i>It is within the controller's legitimate interests to prevent and detect fraud, to consult and input into a database for the purpose of the approval, monitoring and recovery of risks, credit transactions and recurring billing services, through the sharing of both positive information and information on defaults. This processing may be managed by service providers with capital and credit solvency subject to compliance with these rules.</i></p>
--	--

<p><i>Justification</i></p> <p>Experience in practice has shown that these provisions often do not permit the processing of data for fraud prevention and detection purposes. Detecting and preventing fraud is of paramount importance for data controllers. Not only for the controller in question but also to protect data subjects from, for example, falling victim to a loan fraudulently being taken out in their name. Fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.</p> <p>Credit reports should also be explicitly recognised as a legitimate purpose for data processing. The Judgement of the Court of Justice of the European Union in joined Cases C 468/10 and C 469/10 established the presumption in favour of the legitimate interest in cases where the data come from public sources when considering the possible violation of fundamental rights. With regard to fraud prevention files and credit reports, the prevention of fraud, defaults, and over-indebtedness of families are legitimate interests of operators, most notably in the cases of compliance with the rules on responsible lending. Each country has regulated these purposes differently. The above points legitimise the need to include these assumptions within the cases of data processing based on legitimate interest.</p>
--

Amendment 4 – Significant imbalance
Article 7 (4)

Original wording	Proposed amendment
<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><i>Deleted.</i></p>

<p><i>Justification</i></p> <p>What can be considered as a “significant imbalance” or “free” consent will be subject to differing national interpretations. It is essential that this provision does not result in the inability for businesses to process data because an automatic presumption of an imbalance between the positions of the consumer and business within every relationship between the two parties.</p> <p>To avoid legal uncertainty, paragraph 4 should be deleted or at least amended to ensure that where consent cannot provide a legal basis due to an imbalance, the controller can process the data in accordance with another legal basis, as set out in Article 6(1) of the Proposal.</p>
--

Amendment 5 – Right to be forgotten

Article 17(3) introduction

Original wording	Proposed amendment
3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:	3. The controller shall carry out the erasure without unreasonable delay, except to the extent that the retention and dissemination of the personal data is necessary:

Justification

Where controllers are subject to a legal obligation to retain and process data, they may also be obliged to transfer this data to relevant supervisory authorities, such as suspicious transaction reports to financial intelligence units in the context of anti-money laundering rules. Therefore further dissemination should be possible. The “without delay” requirement must be qualified to ensure that it is realistic.

Amendment 6 – Data portability

Article 18

Original wording	Proposed amendment
1. [...] 2. [...] 3. [...]	Deleted.

Justification

Article 15 of the Regulation already provides the right of data subjects to access personal data and to obtain communication thereon, i.e. to obtain a copy. Article 18(1) is therefore a repetition and redundant.

Data portability could be open to abuse, as an ill-intended applicant borrower may alter the data in between receiving, for example, his credit history from one processor and presenting it to a lender. The receiving processor would thus not be able to rely on the accuracy of the data. Data may not be stored or processed in the same language, according to the same categories or procedures. This may render data portability of little value. There is also a risk that this provision could require organisations to disclose trade secrets, internal know-how or information on other customers. We are also concerned that data portability may increase the risk of disclosure of personal data to third parties.

In the specific context of credit data, the European Commission’s Expert Group on Credit Histories decided that it should be left to each individual lender to decide which data access model offers the most convenient and cost-effective solution to data portability. The obligation for data portability would not be in line with these findings. Perhaps there may also be the risk that the receiving processor will require the data subject to provide all his data (history) before offering services. This could be disproportionate.

Where data is made portable, the requirements and obligations for the receiving controller are unclear. For example, does the retention period start again at zero? If deletion is not possible, the scope of the article should be narrowed down to only those sectors where this could appropriately be implemented, e.g. social networks.

Amendment 7 – Automated processing

Article 20(2)(a)

Original wording	Proposed amendment
<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p>	<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p>

Justification

A customer may enquire as to the terms and conditions for entering into, for example, a consumer credit contract. In order for the consumer credit provider to provide information on the APRC, it will assess the consumer's creditworthiness, a legal obligation. Requiring a formal request for the entering into a contract to be proven, would essentially render service and goods providers unable to respond to information requests.

Amendment 8 – Automated processing
Article 20(2)(b)

Original wording	Proposed amendment
<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p>	<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 if the processing:</p> <p>(b) is necessary to comply with a Union or Member State law; or</p>

Justification

It cannot be the task of data controllers to check, whether the Member State law "lays down suitable measures to safeguard the data subject's legitimate interests". On the contrary, firms have to be able to rely on the law.

We would be pleased to answer any question you may have on these elements or to provide you with further information. Please do not hesitate to contact Eurofinas legal adviser Anke Delava (a.delava@eurofinas.org, T: +32 2 778 05 73).