eurofinas

SPECIALISED CONSUMER CREDIT PROVIDERS IN EUROPE

Eurofinas proposals for amendments on the Commission's Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012) 11 final)

October 2012

ABOUT EUROFINAS

Eurofinas, the European Federation of Finance House Associations, is the voice of the specialised consumer credit providers in the EU. As a Federation, Eurofinas brings together associations throughout Europe that represent finance houses, universal banks, specialised banks and captive finance companies of car, equipment, etc. manufacturers. The scope of products covered by Eurofinas members includes all forms of consumer credit products such as personal loans, linked credit, credit cards and store cards. Consumer credit facilitates access to assets and services as diverse as cars, education, furniture, electronic appliances, etc. It is estimated that together Eurofinas members financed over 328 billion Euros worth of new loans during 2011 with outstandings reaching 821 billion Euros at the end of the year.

Eurofinas is entered into the EC Register of Interest Representatives with ID n° 83211441580-56

General Observations

Eurofinas believes that the Commission's Proposal for a General Data Protection Regulation[1] provides a good starting point to further discussions and debate on the EU framework for the protection of personal data.

Although we appreciate that this Proposal is a horizontal instrument applicable across sectors, we feel that a number of aspects are ill-suited for financial services, and in particular consumer credit. We believe it is critical to ensure that the framework would also be workable and efficient for highly regulated sectors such as consumer credit providers, taking into account their operational functioning, key features and the data processing they must carry out in accordance with other legislation.

Against this backdrop, Eurofinas would like to draw your attention to some suggested amendments, which we believe are essential to ensure that lenders can adhere to the aforementioned legislation and carry out sound and responsible lending practices when adopting the new legislative proposal.

The document in hand should be read in conjunction with the March 2012 Eurofinas observations on the Commission's Proposal[2] as well as the work the Federation has recently conducted together with ACCIS on fraud and consumer lending resulting in the release of a report on fraud prevention and data protection (available here).

We would be pleased to answer any question you may have on these elements. Feel free to contact Eurofinas legal adviser Anke Delava (a.delava@eurofinas.org, T: +32 2 778 05 73).

[1] *European Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012) 11 final).*
[2] See *http://www.eurofinas.org/uploads/documents/positions/Eurofinas%20observations%20-%20final.pdf*.

Summary of concerns and suggested amendments

Proposal for a General Data Protection Regulation

Priority concerns:

Data minimisation – Amendment 6, 8 and 49

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.

Lawfulness of processing – Amendment 10

Article 6(1)(c) should be widened-up to include also the requirements of supervisory authorities.

Fraud prevention and detection – Amendment 11, 14, 15, 38

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.

Fraud databases – Amendment 20

In some Member States credit and financial institutions can set up databases which contain data on fraud committed against consumer credit providers. Processing and sharing of this data with other providers is permitted in order to allow credit providers to prevent fraud and minimise risks. To ensure that these databases, whose existence is essential to protect both consumers and businesses, can continue to exist and operate, this provision should reflect the rules currently in place (Article 8(7) of Directive 95/46/EC).

Definition of consent – Amendment 1, 2

The current definition of the data subject's consent requires more clarification. The word "explicit" should be deleted. Consent given by the data subject in a tacit way should be allowed, and therefore the definition should also cover a tacit consent.

Burden of proof for consent – Amendment 16

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.

Withdrawal of consent – Amendment 17

Data controllers will need to process data even after the withdrawal of consent by the data subject, in order to, for example, continue the contractual relationship that may exist between the controller and the subject, as well as allowing for the fulfillment of any obligation on the part of the controller incurred at the request of or under a contract with the data subject. Therefore, where consent has been withdrawn, the continued processing in accordance with another legal basis, as set out in Article 6(1) of the Proposal should be permitted.

Significant imbalance – Amendment 18 and 19

What can be considered as a "significant imbalance" or "free" consent will be subject to differing national interpretations. This provision should 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. 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 should be permitted to process the data in accordance with another legal basis, as set out in Article 6(1) of the Proposal.

Provision free of charge – Amendment 23 and 24

The provision of data held within a database has a cost. Requesting an appropriate (not for profit) contribution from data subjects for data access is critical in deterring fraudsters from obtaining high volumes of consumers' credit data. If data access upon request were to become free of charge then consumers would face an increased risk of frauds (e.g. 'account takeover') with its attendant detrimental consequences.

Publicly available data – Amendment 28

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.

Right to be forgotten and to erasure – Amendment 31 and 32

The article is designed to protect internet social media users. However, it is difficult to execute for example in the financial sector. The data controllers in, for example, the financial sector are obliged to store some data and therefore they are not able to erase all the data processed on the request of the data subject.

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.

Automated decisions – Amendment 39-47

Art. 20 concerns automated processing. The title of this article should therefore be amended to "Measures based on automated processing." Art. 20(1) should retain the reference to "creditworthiness" introduced under Directive 95/46/EC and is preferable to "economic situation."

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.

Implementing acts – Amendment 36, 51 and 86

The aim of the Proposal is to introduce a new European framework for data protection that ensures protection of individual's rights and the free movement of data (Article 1), not to standardise processing systems. We strongly oppose any standardisation of IT solutions and technical systems used by controllers to process data, through the adoption of implementing measures.

Delegated acts – Amendment 13, 33, 44, 50, 58, 62, 82-85

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to "non-essential" aspects of the Regulation, rather than, as in the Proposal, on all essential aspects of the Regulation.

The Regulation should therefore not be subject to change in particular on the following issues:

- Lawfulness of processing;
- Right to be forgotten;
- Measures based on profiling;

- Design;
- Communication of personal data breach;
- Data protection impact assessment.

Further key concerns:

Groups of undertakings – Amendment 4

The definition of a 'group of undertakings' in Art 4(16) as a controlling undertaking and its controlled undertakings is too narrow and it should be expanded to any group of companies or another comparable economic grouping. A level playing field should be guaranteed to all kind of groups of undertakings.

Principles relating to personal data processing – Amendment 5, 7 and 8

"In a transparent manner" is vague, legally uncertain and redundant, as Article 11 and 14 of the Proposal already require controllers to have transparent and accessible policies and to provide data subjects with substantive information. This should therefore be deleted, reverting back to the wording of Directive 95/46/EC.

The "without delay" requirement must be qualified to ensure that it is realistic.

Further processing – Amendment 5

Article 5(b) and Article 6(4), are contradictory with regard to further processing for purposes incompatible with the purpose for which the data was collected. To clarify the relation between the two Articles and increase legal certainty, Article 5(b) should be rephrased so as to specify that personal data must not be further processed in a way incompatible with the purposes for which it has been collected, unless specific provisions of the regulation provide otherwise.

Specific purposes – Amendment 9

In some Member States, consumers give explicit consent for the processing of their data for general purposes. If explicit consent were to be required for each separate purpose, this would be disproportionately time-consuming, resource-intensive and costly. It is therefore proposed to align the wording with Directive 95/46/EC, currently already in force in the Member States.

Basis provided for in law – Amendment 12 and 32

Whilst it is the responsibility of the Member States to ensure that their national legislation meets the above requirements, data controllers would bear the risks when processing data in accordance with a potentially non-conforming law. This should be avoided to increase legal certainty for controllers and processors.

Providing information electronically – Amendment 21 and 22

The requirement to provide information in electronic form raises concerns about the security of the data. It is not current practice in credit markets. An email request does not enable a lender to validate that the request is from the data subject as there is no guarantee that it will be secure. It would also be a considerable challenge to take appropriate technological measures to ensure security of the data in a way that would work for every customer.

Contract terms and general conditions – Amendment 25

The information to be provided to data subjects shall be an exhaustive list, to ensure that controllers have legal certainty with regard to their information obligations. Data subjects will already have been provided the contract terms and conditions when they signed this contract. The duplication of such a requirement would lead to overloading consumers with information.

Storage period – Amendment 26, 29, 30

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.

Information to the data subject – Amendment 27

The term "disproportionate effort" is open to various interpretations and should be clarified.

Right to data portability – Amendment 34 - 37

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.

The imposition of technical requirements to enable personal data to become portable, would come at a significant cost for businesses.

Responsibility of the controller – Amendment 48

Introducing an obligation to have the verification carried out by internal/external auditors would introduce an unnecessary duplication of the measures taken by controllers to ensure compliance and an unjustified expense. It should be left to controllers to decide and assess what steps need to be taken to verify adherence to the Regulation.

Processor – Amendment 52-54

The scope of some of the provisions of Article 26 is unclear or repeat obligations already contained in other articles.

Processing under the authority of the controller and processor – Amendment 55

The exemption should not only cover situations where the data processor or the person acting under the authority of the controller or of the processor who has access to personal data is required to process personal data, but also situations where they have the right to process data under the national or EU legislation.

Notification of a personal data breach – Amendment 56, 57, 59

An appropriate time period should be foreseen for notifying the supervisory authority of the substantial amount of information required in Article 31(3) regarding data breaches which are likely to substantially adversely affect data subjects.

In some Member States, credit and financial institutions shall notify the Financial Services Authority where substantial disruptions in services provided to the customers and in payment and IT systems occur. Where such an obligation already exists in national law, this should not be duplicated by an additional obligation to

also notify the data protection supervisor. This sectoral supervisor should instead notify the data protection supervisor.

Data subjects should be informed of a breach where there could be a significant impact on them.

Data Protection Impact Assessment – Amendment 60

Data processors cannot and should not be asked to make the assessment as to whether or not a legal obligation placed upon them poses "a high degree of specific risks". This is a consideration for the legislator and, at European level, through the opinion of the European Data Protection Supervisor, who advises the Institutions on legislation that affects privacy.

Views of data subjects –Amendment 61

It will be impossible to implement in practice and data subjects' representatives may not always have the expertise, qualifications or resources to respond to such imposed requests for their views. The supervisory authority will be in better qualified to respond to such requests.

Data Protection Officer – Amendment 63

This provision will prevent someone being replaced in the normal course of the management of a company and its employees. This is particularly pertinent for smaller companies where the data protection officer may well be only part of the individual's job designation. There has to be flexibility for the firm to be able to reorganise and reshape its employee resources. The officer should be no different position from any other person in a compliance function as far as these issues are concerned.

Transfers by way of appropriate safeguards – Amendment 64--66

The reference to the processor or controller restricts the authorisation to them as the only appropriate parties to provide guarantees for the performance of the international data transfer to a third country, eliminating others such as the importer of the data.

We included as appropriate guarantees the binding declaration of the international organisation or corporate group acting as data importer as an alternative instrument to further facilitate international data flows, thereby avoiding directly subordinating the legality of the transfer to the signing of a contract between the parties, and therefore, the development of multiple contract terms with each of the exporters.

Said declarations could incorporate such elements as the Commission deems necessary in order to safeguard the right to privacy of the citizens of the European Union, in addition to the development of the principle of international cooperation laid down in Article 45(1) of the Regulation.

Derogations to transfer by way of adequacy decision or appropriate safeguards – Amendment 67--69

The reference to the processor or controller restricts the authorisation to them as the only appropriate parties to provide guarantees for the performance of the international data transfer to a third country, eliminating others such as the importer of the data.

Given the new regime for data processors, which includes:
(i) A written contract between the parties governing the mandated processing of personal data.
(ii) The obligation of the controller to select a processor that offers sufficient guarantees that the processing will be tailored to the provisions of these rules,
(iii) The documentation of the entire process (art. 28) with details of processing, transfers, documentation, guarantees adopted in the event of transfers, and
(iv) The requirement that this documentation is made available to the supervisory authority,
It should be possible to transfer data in these cases.

Where an activity is conducted subject to specific regulation and supervision, including financial and banking or insurance services, the approval process in these cases should also be exempted given the guarantee that the processing in such activities is subject to regulation and the legitimacy thereof.

Supervisory authorities – Amendment 70--72

The principle of concentration of functions preached by this article should apply in the case of branches and subsidiary companies, affiliates and investees of a parent company, since they share the same foundation.

We understand that it is essential that the supervisory authority support those responsible for compliance with the rules and most especially the Data Protection Officers, in terms of training, information and cooperation to increase the level of compliance with the regulation.

The free services of the supervisory authority must exist regardless of the party requesting it.

Consistency mechanism – Amendment 73

We understand that the consistency mechanism should also be able to be activated by a controller or processor directly or indirectly affected by the measure on which the request applies or any other accredited third party with a legitimate interest in confirming the adequacy of country-level measures applied by a supervisory authority.

Collective redress – Amendment 74, 75

We are opposed to the introduction of class action mechanisms at European level, especially through sector specific legislation. It has not been shown that the absence of such mechanisms has prevented data subjects from exercising their rights.

Sanctions – Amendment 76 - 81

Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

The written warning is a persuasive tool which must be used by the supervisory authority the times and where it deems appropriate. In keeping with the spirit and purpose of the Regulation, only intentional non-compliance or impairment of the principles and rights set forth in the Regulation should be subject to financial penalty.

CHAPTER II – Principles

Amendment 1
Article 4(8)

Original wording	Proposed amendment
For the purposes of this Regulation: (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;	For the purposes of this Regulation: (8) 'the data subject's consent' means any freely given specific, informed, explicit ***or tacit*** 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;

Justification

The current definition of the data subject's consent requires more clarification. The word "explicit" should be deleted. Consent given by the data subject in a tacit way should be allowed, and therefore the definition should also cover a tacit consent.

Amendment 2
***Recital 25* – the accompanying recital to Article 4(8)**

Original wording	Proposed amendment
Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	Consent should be given explicitly ***or tacitly*** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Justification
See justification amendment 1.

Amendment 3
Article 4(16)

Original wording	Proposed amendment
For the purposes of this Regulation: (16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	For the purposes of this Regulation: (16) 'group of undertakings' means a controlling undertaking and its controlled undertakings***; the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.;***

Justification
The definition of a 'group of undertakings' in Art 4(16) as a controlling undertaking and its controlled undertakings is too narrow and it should be aligned to recital 28. A level playing field should be guaranteed to all kind of groups of undertakings.

Amendment 4
Article 5(a)

Original wording	Proposed amendment
Personal data must be: (a) processed lawfully, fairly **and in a transparent manner in relation to the data subject**;	Personal data must be: (a) processed lawfully ***and*** fairly;

Justification
"In a transparent manner" is vague, legally uncertain and redundant, as Article 11 and 14 of the Proposal already require controllers to have transparent and accessible policies and to provide data subjects with substantive information. This should therefore be deleted, reverting back to the wording of Directive 95/46/EC.

Amendment 5
Article 5(b)

Original wording	Proposed amendment
Personal data must be: (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;	Personal data must be: (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes ***unless provisions of this Regulation provide otherwise****;*

Justification

Article 5(b) and Article 6(4), are contradictory with regard to further processing for purposes incompatible with the purpose for which the data was collected. To clarify the relation between the two Articles and increase legal certainty, Article 5(b) should be rephrased so as to specify that personal data must not be further processed in a way incompatible with the purposes for which it has been collected, unless specific provisions of the regulation provide otherwise.

Amendment 6
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 7
Article 5(d)

Original wording	Proposed amendment
Personal data must be: (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;	Personal data must be: (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 ***unreasonable*** delay;

Justification
The "without delay" requirement must be qualified to ensure that it is realistic.

Amendment 8
Recital 30 – the accompanying recital to Article 5

Original wording	Proposed amendment
Any processing of personal data should be lawful, fair **and transparent in relation to the individuals concerned**. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and **limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are** not excessive **and that the period for which the data are stored is limited to a strict minimum**. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.	Any processing of personal data should be lawful ***and*** fair. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and not excessive. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Justification
See justification amendments 4-7.

Amendment 9
Article 6(1)(a)

Original wording	Proposed amendment
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;	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 purposes;

Justification

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. It is therefore proposed to align the wording with Directive 95/46/EC, currently already in force in the Member States.

Amendment 10
Article 6(1)(c)

Original wording	Proposed amendment
1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (c) processing is necessary for compliance with a legal obligation to which the controller is subject;	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (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;***

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 11
Article 6(1)(f)

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

Justification

The lawfulness of processing based on the legitimate interest must be extended to legitimate interests pursued by third parties to whom the data are disclosed by a controller. To exclude this provision might compromise an essential principle of legitimacy that is very important in the market. It would be contradictory to admit this principle with reference to the controller itself but not with reference to another party (the second controller) receiving data from the former. The result would be

to exclude the possibility for data suppliers to supply on a legitimate basis data to final users of such data even if the legitimate interest is recognised and justified. The limitation is not reasonable and only has the effect to limit the market without providing greater protection for data subjects.

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.

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.

Amendment 12
Article 6(3)

Original wording	Proposed amendment
3. Processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (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.**	3. Processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject.

Justification

Whilst it is the responsibility of the Member States to ensure that their national legislation meets the above requirements, data controllers would bear the risks when processing data in accordance with a potentially non-conforming law. This should be avoided to increase legal certainty for controllers and processors.

In any case, as privacy is a fundamental right, national courts do not need this explicit reference in order to assess whether a law allowing for data protection impedes upon a fundamental right.

Amendment 13
Article 6(5)

Original wording	Proposed amendment
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.	***Deleted***

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to "non-essential" aspects of the Regulation. What constitutes a "legitimate interests pursued by controllers" cannot be seen as non-essential.

Amendment 14
Recital 31 – the accompanying recital to Article 6

Original wording	Proposed amendment
In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.	In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, ***for example to detect and prevent fraud,*** laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.

Justification

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.

Amendment 15
Recital 38 – the accompanying recital to Article 6

Original wording	Proposed amendment
The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	The legitimate interests of a controller, **such as fraud prevention and detection,** may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.

Justification

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.

Amendment 16
Article 7(1)

Original wording	Proposed amendment
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.	***Deleted.***

Justification

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.

Amendment 17
Article 7(3)

Original wording	Proposed amendment
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.	3. The data subject shall have the right to withdraw his or her consent at any time. ***Without prejudice to Article 6(1)***, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Justification

Data controllers will need to process data even after the withdrawal of consent by the data subject, in order to, for example, continue the contractual relationship that may exist between the controller and the subject, as well as allowing for the fulfillment of any obligation on the part of the controller incurred at the request of or under a contract with the data subject.

Therefore, where consent has been withdrawn, the continued processing in accordance with another legal basis, as set out in Article 6(1) of the Proposal should be permitted.

Amendment 18
Article 7 (4)

Original wording	Proposed amendment
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.	***Deleted.***

Justification

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.

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.

Amendment 19
Recital 34 – the accompanying recital to Article 7

Original wording	Proposed amendment
(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject. **These processors and controllers should instead rely on another legal ground for processing data.**

Justification

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.

Where consent cannot provide a legal basis due to an imbalance, the controller should be permitted to process the data in accordance with another legal basis, as set out in Article 6(1) of the Proposal.

Amendment 20
Article 9(1)

Original wording	Proposed amendment
1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life **or criminal convictions or related security measures** shall be prohibited.	1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life shall be prohibited.

Justification

In some Member States credit and financial institutions can set up databases which contain data on fraud committed against consumer credit providers. Processing and sharing of this data with other providers is permitted in order to allow credit providers to prevent fraud and minimise risks.

To ensure that these databases, whose existence is essential to protect both consumers and businesses, can continue to exist and operate, this provision should reflect the rules currently in place (Article 8(7) of Directive 95/46/EC).

CHAPTER III – Rights of the Data Subject

Section 1 – Transparency and Modalities

Amendment 21
Article 12(1)

Original wording	Proposed amendment
1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. ***Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.***	1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19.

Justification

The requirement to provide information in electronic form raises concerns about the security of the data. It is not current practice in credit markets. An email request does not enable a lender to validate that the request is from the data subject as there is no guarantee that it will be secure. It would also be a considerable challenge to take appropriate technological measures to ensure security of the data in a way that would work for every customer.

Amendment 22
Article 12(2)

Original wording	Proposed amendment
2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for ***a* further month**, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. **Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.**	2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for ***another eight weeks***, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing.

Justification Where the validity of contested data has to be verified with third parties it seems appropriate to extend this period by another eight weeks. The requirement to provide information in electronic form raises concerns about the security of the data. It is not current practice in credit markets. An email request does not enable a lender to validate that the request is from the data subject as there is no guarantee that it will be secure. It would also be a considerable challenge to take appropriate technological measures to ensure security of the data in a way that would work for every customer.

Amendment 23
Article 12(4)

Original wording	Proposed amendment
4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.	4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, ***their complexity or the total number of requests,*** the controller may charge a**n** ***appropriate*** fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

Justification The provision of data held within a database has a cost. Requesting an appropriate (not for profit) contribution from data subjects for data access is critical in deterring fraudsters from obtaining high volumes of consumers' credit data. If data access upon request were to become free of charge then consumers would face an increased risk of frauds (e.g. 'account takeover') with its attendant detrimental consequences.

Amendment 24
Recital 47 – the accompanying recital to Article 12

Original wording	Proposed amendment
Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request**, free of charge**, in particular access to	Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request in particular access to data, rectification, erasure

data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.	and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.

Justification

The provision of data held within a database has a cost. Requesting an appropriate (not for profit) contribution from data subjects for data access is critical in deterring fraudsters from obtaining high volumes of consumers' credit data. If data access upon request were to become free of charge then consumers would face an increased risk of frauds (e.g. 'account takeover') with its attendant detrimental consequences.

Section 2 – Information and Access to Data

Amendment 25
Article 14(1)(b)

Original wording	Proposed amendment
1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with ***at least*** the following information: (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);	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following information: (b) the purposes of the processing for which the personal data are intended, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

Justification

The information to be provided to data subjects shall be an exhaustive list, to ensure that controllers have legal certainty with regard to their information obligations.

Data subjects will already have been provided the contract terms and conditions when they signed this contract. The duplication of such a requirement would lead to overloading consumers with information.

Amendment 26
Article 14(1)(c)

Original wording	Proposed amendment
1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with **at least** the following information: (c) the period for which the personal data will be stored;	1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following information: ***Deleted****;*

Justification

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 27
Article 14(5)(b)

Original wording	Proposed amendment
5. Paragraphs 1 to 4 shall not apply, where: (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	5. Paragraphs 1 to 4 shall not apply, where: (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort, ***such as substantial manual work***; or

Justification
The term "disproportionate effort" is open to various interpretations and should be clarified.

Amendment 28
Article 14(5)(e) - new

Original wording	Proposed amendment
-	5. Paragraphs 1 to 4 shall not apply, where: (e) the data are not collected from the data subject and ***are publicly available.***

Justification
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.

Amendment 29
Recital 48 – the accompanying recital to Article 14

Original wording	Proposed amendment
The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, **how long the data**	The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, on the existence of

will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.	the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

Justification

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 30
Article 15(1)(d)

Original wording	Proposed amendment
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: **d) the period for which the personal data will be stored;**	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: ***d) Deleted*.**

Justification

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.

Section 3 – Rectification and Erasure

Amendment 31
Article 17(1)(a)

Original wording	Proposed amendment
1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;	1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed ***and when the data controller has no legal or regulatory ground to retain the data***;

Justification
The article is designed to protect internet social media users. However, it is difficult to execute for example in the financial sector. The data controllers in, for example, the financial sector are obliged to store some data and therefore they are not able to erase all the data processed on the request of the data subject.

Amendment 32
Article 17(3)

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: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; **Member State**	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***:*** (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law

laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; (e) in the cases referred to in paragraph 4.	to which the controller is subject; (e) in the cases referred to in paragraph 4.

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.

Whilst it is the responsibility of the Member States to ensure that their national legislation meets the above requirements, data controllers would bear the risks when processing data in accordance with a potentially non-conforming law. This should be avoided to increase legal certainty for controllers and processors.

Amendment 33
Article 17(9)

Original wording	Proposed amendment
9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying: (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	***Deleted***

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to "non-essential" aspects of the Regulation. Laying down a new body of detailed rules for specific sectors cannot be considered as non-essential.

Amendment 34
Article 18(1)

Original wording	Proposed amendment
1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.	***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.

Amendment 35
Article 18(2)

Original wording	Proposed amendment
2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.	***Deleted***

Justification
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 36
Article 18(3)

Original wording	Proposed amendment
3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***Deleted***

Justification Standardisation of IT solutions and technical systems used by controllers to process data should not be the aim of the new data protection framework. The imposition of technical requirements to enable personal data to become portable, would come at a significant cost for businesses. 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.

Amendment 37
Recital 55 – the accompanying recital to Article 18

Original wording	Proposed amendment
To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are	***Deleted***

processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.	

Justification

See justification in amendments 34-36.

Section 4 – Right to Object and Profiling

Amendment 38
Article 19(1)

Original wording	Proposed amendment
1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.	1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject***, such as the processing of data for the prevention of fraud and for credit reports***.

Justification
See justification amendment 11.

Amendment 39
Article 20 - Title

Original wording	Proposed amendment
Measures based on ***profiling***	Measures based on ***automated processing***

Justification
Art. 20 concerns automated processing. The title of this article should therefore be amended to "Measures based on automated processing."

Amendment 40
Article 20(1)

Original wording	Proposed amendment
1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and	1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and

which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, **economic situation,** location, health, personal preferences, reliability or behaviour.	which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person***, such as his creditworthiness,*** or to analyse or predict in particular the natural person's performance at work, location, health, personal preferences, reliability or behaviour.

Justification

Art. 20(1) should retain the reference to "creditworthiness" introduced under Directive 95/46/EC and is preferable to "economic situation."

Amendment 41
Article 20(2)(a)

Original wording	Proposed amendment
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: (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	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: (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

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 42
Article 20(2)(b)

Original wording	Proposed amendment
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: […] (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 […]	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: […] (b) is ***necessary to comply with*** a Union or Member State law; or […]

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.

Amendment 43
Article 20(4)

Original wording	Proposed amendment
4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 **and the envisaged effects of such processing on the data subject**.	4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1.

Justification

It may not always be possible to determine in advance the envisaged effects, in particular where automated processing is subject to subsequent human intervention. An explanation of the existence of this measure will adequately inform and protect data subjects.

Amendment 44
Article 20(5)

Original wording	Proposed amendment
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.	***Deleted***

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to "non-essential" aspects of the Regulation. Laying down a new body of detailed rules for specific sectors cannot be considered as non-essential.

Furthermore, similar provisions on automated processing have been in place since Directive 95/46/EC. Controllers and processors have built systems which rely on the interpretations of these rules already in place. Laying down new rules without any specific justification would create legal uncertainty.

Amendment 45
Recital 58 – the accompanying recital to Article 20

Original wording	Proposed amendment
Every natural person should have the right not to be subject to a measure which is based on **profiling by means of** automated processing. **However,** such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.	Every natural person should have the right not to be subject to a measure which is based ***solely*** on automated processing. Such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.

Justification

This recital should reflect the corresponding article with regard to the content.

Amendment 46
Recital 51

Original wording	Proposed amendment
Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing **and what might be, at least when based on profiling, the consequences of such processing**. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data ***and*** what is the logic of the data that are undergoing the processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.

Justification
See justification to amendment 43.

Amendment 47
Recital 59

Original wording	Proposed amendment
Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on **profiling**, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or	Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on ***automated processing***, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of

of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.	the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Justification

See justification to amendment 39.

CHAPTER IV – Controller and Processor

Section 1 – General Obligations

Amendment 48
Article 22(3)

Original wording	Proposed amendment
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. **If proportionate,** this verification **shall be** carried out by independent internal or external auditors.	3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. ***Controllers may have*** this verification carried out by independent internal or external auditors.

Justification

Introducing an obligation to have the verification carried out by internal/external auditors would introduce an unnecessary duplication of the measures taken by controllers to ensure compliance and an unjustified expense. It should be left to controllers to decide and assess what steps need to be taken to verify adherence to the Regulation.

Amendment 49
Article 23(2)

Original wording	Proposed amendment
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the **minimum** necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

Justification

See justification amendment 6**.**

Amendment 50
Article 23(3)

Original wording	Proposed amendment
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.	***Deleted.***

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to "non-essential" aspects of the Regulation. Laying down a new body of detailed rules for specific sectors cannot be considered as non-essential.

Amendment 51
Article 23(4)

Original wording	Proposed amendment
4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	***Deleted***

Justification

The aim of the Proposal is to introduce a new European framework for data protection that ensures protection of individual's rights and the free movement of data (Article 1), not to standardise processing systems, as proposed in Article 23(4). We strongly oppose any standardisation of IT solutions and technical systems used by controllers to process data, through the adoption of implementing measures.

Amendment 52
Article 26(2)(a)

Original wording	Proposed amendment
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall: (a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;	2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall: ***(a) Deleted***

Justification
The scope of this provision is unclear.

Amendment 53
Article 26(2)(f)

Original wording	Proposed amendment
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall: (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall: ***(f) Deleted***

Justification
Obligations to adhere to these respective articles is already contained in other parts and there is thus no need to repeat these.

Amendment 54
Article 26(3)

Original wording	Proposed amendment
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.	***Deleted***

Justification
Obligations of the processor regarding the instructions of the controller and the obligations of the processor are already contained in other sections, so it is repetitive.

Amendment 55
Article 27

Original wording	Proposed amendment
The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless **required** to do so by Union or Member State law.	The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless ***authorised*** to do so by Union or Member State law.

Justification
The exemption should not only cover situations where the data processor or the person acting under the authority of the controller or of the processor who has access to personal data is required to process personal data, but also situations where they have the right to process data under the national or EU legislation.

Section 2 – Data Security

Amendment 56
Article 31(1)

Original wording	Proposed amendment
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 ***which is likely to substantially adversely affect the personal data or privacy of the data subject***, the controller shall notify the personal data breach to the supervisory authority ***within a reasonable period of time.*** The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within ***a reasonable period of time***. ***For regulated activities, where a duty already exists to notify a personal data breach to sectoral supervisory authorities, the latter shall communicate the personal data breach to the data protection supervisory authority.***

Justification

An appropriate time period should be foreseen for notifying the supervisory authority of the substantial amount of information required in Article 31(3) regarding data breaches which are likely to substantially adversely affect data subjects.

In some Member States, credit and financial institutions shall notify the Financial Services Authority where substantial disruptions in services provided to the customers and in payment and IT systems occur. Where such an obligation already exists in national law, this should not be duplicated by an additional obligation to also notify the data protection supervisor. This sectoral supervisor should instead notify the data protection supervisor.

Amendment 57
Article 32(1)

Original wording	Proposed amendment
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.	1. When the personal data breach is likely to ***substantially*** 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.

Justification Data subjects should be informed of a breach where there could be a significant impact on them.

Amendment 58
Article 32(5)

Original wording	Proposed amendment
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.	***Deleted***

Justification The establishment by the Commission at a later stage of the requirements for these circumstances is likely to create substantial legal uncertainty.

Amendment 59
Recital 67 – the accompanying recital to Article 31 & 32

Original wording	Proposed amendment
A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority **without undue delay and, where feasible, within 24 hours**. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The	A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach, ***which substantially adversely affects the personal data or privacy of the data subject,*** has occurred, the controller should notify the breach to the supervisory authority ***within a reasonable period of time.*** Where this cannot achieved within ***a reasonable period of time***, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be ***substantially*** adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data

notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.	subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

Justification

See justification for amendment 56 & 57.

Section 3 – Data Protection Impact Assessment and Prior Authorisation

Amendment 60
Article 33(2)(a)

Original wording	Proposed amendment
2. The following processing operations in particular present specific risks referred to in paragraph 1: (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;	2. The following processing operations in particular present specific risks referred to in paragraph 1: (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual, ***except where this systematic and extensive evaluation is a legal obligation for the controller provided for by Union or Member State law***;

Justification

Data processors cannot and should not be asked to make the assessment as to whether or not a legal obligation placed upon them poses “a high degree of specific risks”. This is a consideration for the legislator and, at European level, through the opinion of the European Data Protection Supervisor, who advises the Institutions on legislation that affects privacy.

Amendment 61
Article 33(4)

Original wording	Proposed amendment
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.	4. The controller shall seek the views of ***the supervisory authority*** on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

Justification

It will be impossible to implement in practice and data subjects’ representatives may not always have the expertise, qualifications or resources to respond to such imposed requests for their views. The

supervisory authority will be in better qualified to respond to such requests.

Amendment 62
Article 33(6)

Original wording	Proposed amendment
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.	***Deleted***

Justification Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to "non-essential" aspects of the Regulation.

Amendment 63
Article 35(7)

Original wording	Proposed amendment
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.	***Deleted***

Justification This provision will prevent someone being replaced in the normal course of the management of a company and its employees. This is particularly pertinent for smaller companies where the data protection officer may well be only part of the individual's job designation. There has to be flexibility for the firm to be able to reorganise and reshape its employee resources. The officer should be no different position from any other person in a compliance function as far as these issues are concerned.

CHAPTER V – Transfer of Personal Data to Third Countries or International Organisations

Amendment 64
Article 42(1)

Original wording	Proposed amendment
1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if **the controller or processor has adduced** appropriate safeguards with respect to the protection of personal data in a legally binding instrument.	1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation or corporate group only if appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

Justification

The reference to the processor or controller restricts the authorisation to them as the only appropriate parties to provide guarantees for the performance of the international data transfer to a third country, eliminating others such as the importer of the data.

Amendment 65
Article 42(2)(e) - new

Original wording	Proposed amendment
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:	2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: ***(e) a legally binding statement by the international organisation or corporate group acting as a data importer, through which it is subjected to the fundamental principles of this Regulation, according to the models adopted by the Commission following Article 45(1).*** **(NEW)**

Justification

We included as appropriate guarantees the binding declaration of the international organisation or corporate group acting as data importer as an alternative instrument to further facilitate international data flows, thereby avoiding directly subordinating the legality of the transfer to the signing of a

contract between the parties, and therefore, the development of multiple contract terms with each of the exporters. Said declarations could incorporate such elements as the Commission deems necessary in order to safeguard the right to privacy of the citizens of the European Union, in addition to the development of the principle of international cooperation laid down in Article 45(1) of the Regulation.

Amendment 66
Article 42(3)

Original wording	Proposed amendment
3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) **or** (c) of paragraph 2 shall not require any further authorisation.	3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b), (c) ***or (e)*** of paragraph 2 shall not require any further authorisation.

Justification
See justification amendment 65.

Amendment 67
Article 44(1)(h)

Original wording	Proposed amendment
1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, **which cannot be qualified as frequent or massive,** and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations **and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary**.	1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations

Justification The article presents legal concepts -frequent and massive legitimate interests- whose interpretation may result in greater legal uncertainty than what the wording aims to provide. Furthermore, regardless of this uncertainty, there is no legal basis for applying a different solution in the event that there is a frequent legitimate interest as opposed to an infrequent legitimate interest, considering the impact on the protection of data transfer depends not frequency or size, but rather on the types of processing and data affected.

Amendment 68
Article 44(1)(i) - New

Original wording	Proposed amendment
1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:	1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: ***i) When the transfer is made to a processor following the instructions of a controller located in the European Union. In this case, Articles 26 to 28 and Article 30 concerning the security of the processing will apply; or*** **(new)**

Justification Given the new regime for data processors, which includes: (i) A written contract between the parties governing the mandated processing of personal data. (ii) The obligation of the controller to select a processor that offers sufficient guarantees that the processing will be tailored to the provisions of these rules, (iii) The documentation of the entire process (art. 28) with details of processing, transfers, documentation, guarantees adopted in the event of transfers, and (iv) The requirement that this documentation is made available to the supervisory authority, It should be possible to transfer data in these cases.

Amendment 69
Article 44(1)(j) - new

Original wording	Proposed amendment
1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate	1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate

safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:	safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: ***j) When the international transfer is made within the framework of the development of an activity subject to specific regulation and supervision by a recognised or established regulator in the European Union, provided that the transfer is performed in accordance with said legislation and within the scope of the activity being supervised. (new)***

Justification

Where an activity is conducted subject to specific regulation and supervision, including financial and banking or insurance services, the approval process in these cases should also be exempted given the guarantee that the processing in such activities is subject to regulation and the legitimacy thereof.

CHAPTER VI – Independent Supervisory Authorities

Section 2 – Duties and powers

Amendment 70
Article 51(2)

Original wording	Proposed amendment
2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.	2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor, ***or any subsidiary or affiliate thereof is*** established in more than one Member State, the supervisory authority of the main establishment or parent company of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

Justification

The principle of concentration of functions preached by this article should apply in the case of branches and subsidiary companies, affiliates and investees of a parent company, since they share the same foundation.

Amendment 71
Article 52(3)

Original wording	Proposed amendment
3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulations and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.	3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulations and, if appropriate, co-operate with the supervisory authorities in other Member States to this end. ***The supervisory authority shall advise controllers and processors regarding the obligations thereof, and especially the Data Protection Officers, promoting cooperation, training and permanent contact with them for a better understanding and enforcement of data protection.***

Justification We understand that it is essential that the supervisory authority support those responsible for compliance with the rules and most especially the Data Protection Officers, in terms of training, information and cooperation to increase the level of compliance with the regulation.

Amendment 72
Article 53(5)

Original wording	Proposed amendment
5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.	5. The performance of the duties of the supervisory authority shall be free of charge for the data subject, ***data controller, data processor and Data Protection Officers and be included in the budgets of the supervisory authority.***

Justification The free services of the supervisory authority must exist regardless of the party requesting it.

CHAPTER VII – Co-Operation and Consistency

Section 2 – Consistency

Amendment 73
Article 58(3)

Original wording	Proposed amendment
3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.	3. Any supervisory authority or the European Data Protection Board ***and any third party with accredited legitimate interest*** may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

Justification

We understand that the consistency mechanism should also be able to be activated by a controller or processor directly or indirectly affected by the measure on which the request applies or any other accredited third party with a legitimate interest in confirming the adequacy of country-level measures applied by a supervisory authority.

CHAPTER VIII – Remedies, Liability and Sanctions

Amendment 74
Article 76(1)

Original wording	Proposed amendment
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.	***Deleted***

Justification
We are opposed to the introduction of class action mechanisms at European level, especially through sector specific legislation. It has not been shown that the absence of such mechanisms has prevented data subjects from exercising their rights.

Amendment 75
Recital 112 – the accompanying recital to Article 76

Original wording	Proposed amendment
Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.	***Deleted***

Justification
See justification for amendment 74.

Amendment 76
Article 79(2)

Original wording	Proposed amendment
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.	2. ***Where the supervisory authority decides to impose an administrative sanction, this sanction shall in each individual case be*** effective, proportionate and dissuasive. The amount of ***an*** 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.

Justification

Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

Amendment 77
Article 79(3)

Original wording	Proposed amendment
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:** **(a) a natural person is processing personal data without a commercial interest; or** **(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.**	3. In case of a non-intentional non-compliance with this Regulation, ***or in the event that the breach of an obligation under this Regulation has not caused actual harm or impairment of the principles and rights set out in Chapters II and III of this Regulation***, a warning in writing may be given and no sanction imposed.

Justification

The written warning is a persuasive tool which must be used by the supervisory authority the times

and where it deems appropriate. In keeping with the spirit and purpose of the Regulation, only intentional non-compliance or impairment of the principles and rights set forth in the Regulation should be subject to financial penalty.

Amendment 78
Article 79(4)

Original wording	Proposed amendment
4. The supervisory authority **shall** impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently: […]	4. The supervisory authority ***may*** impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently: […]

Justification Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

Amendment 79
Article 79(5)

Original wording	Proposed amendment
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: […]	5. The supervisory authority ***may*** 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: […]

Justification Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

Amendment 80
Article 79(6)

Original wording	Proposed amendment
6. The supervisory authority **shall** impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: […]	6. The supervisory authority ***may*** 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: […]

Justification

Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

Amendment 81
Recital 119 – the accompanying recital to Article 76

Original wording	Proposed amendment
Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.	***Supervisory authorities shall be empowered to impose administrative sanctions*** to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.

Justification

See justification for amendment 76-80.

CHAPTER X – Delegated Acts and Implementing Acts

Amendment 82
Article 86(2)

Original wording	Proposed amendment
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.	2. The delegation of power referred to in Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 22(4), Article 26(5), Article 28(5), Article 30(3), Article 31(5), 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.

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to "non-essential" aspects of the Regulation, rather than, as in the Proposal, on all essential aspects of the Regulation.

The Regulation should therefore not be subject to change in particular on the following issues:
- Lawfulness of processing (Article 6(5));
- Right to be forgotten (Article 17(9));
- Measures based on profiling (Article 20(5));
- Design (Article 23(4));
- Communication of personal data breach (Article 32(5));
- Data protection impact assessment (Article 33(6)).

Amendment 83
Article 86(3)

Original wording	Proposed amendment
3. 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) may be revoked at any time by the	3. The delegation of power referred to in Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 22(4), Article 26(5), Article 28(5), Article 30(3), Article 31(5), 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) may be revoked at any time by the European Parliament or by the Council. A decision of

European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

Justification

See justification for amendment 82.

Amendment 84
Article 86(5)

Original wording	Proposed amendment
5. A delegated act adopted pursuant to **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 enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.	5. A delegated act adopted pursuant to Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 22(4), Article 26(5), Article 28(5), Article 30(3), Article 31(5), 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 enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Justification

See justification for amendment 82.

Amendment 85

Recital 129 – the accompanying recital to Article 86

Original wording	Proposed amendment
In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of **lawfulness of processing**; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; **the right to be forgotten and to erasure; measures based on profiling;** criteria and requirements in relation to the responsibility of the controller and **to data protection by design and by default**; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, **and on the circumstances where a personal data breach is likely to adversely affect the data subject**; **the criteria and conditions for processing operations requiring a data protection impact assessment**; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.	In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; criteria and requirements in relation to the responsibility of the controller and a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

Justification
See justification for amendment 82.

Amendment 86
Recital 130

Original wording	Proposed amendment
In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the **right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation**; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.	In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

Justification
See justification for amendment 36 and 51.