Microsoft positions and suggestions for the draft *General Data Protection Regulation*

Microsoft positions and concerns at a glance

1/ Microsoft welcomes the draft Regulation, which seeks to better harmonise the EU's data protection regime. Any responsible company has a role to play here. Our approach is based on Trust and Transparency (privacy by design, Office 365 Trust Center: http://Office 365.microsoft.com/).

2/ However the text is too prescriptive: rather than dictate approaches, the Regulation should offer more incentives to trustworthy companies. It is key to motivate companies via the concept of recognised accountability (i.e., to encourage good practices by rewarding organisations that demonstrate responsibility and adopt robust privacy programs including in relation to the transfer of data in the Cloud).

3/ Delegated acts as drafted can create new burdens and uncertainty. We suggest reducing the number of delegated acts.

4/ The concept of administrative fines is appropriate, but the "one-size-fits-all" approach that puts on the same level companies that intentionally cause harm and those that were negligent is disproportionate.

5/ Rules relating to international data transfers and the role of Processors/Controllers need to be adapted to the Cloud context.

6/ Breach notice will drive improved data security across industry. Such rules must be crafted in a way that ensures data subjects pay close attention to notices.

***

Microsoft welcomes efforts to strengthen and harmonise the EU's data protection regime. Our company's greatest asset is customer trust and our technologies are developed with data protection in mind. Our priority is to protect personal data in an age where we have ubiquitous connectivity, pervasive online business and social networking, and flows and storage of information all over the world on all kinds of computers and devices.

As we know from our direct experience, the challenge before us lies in protecting Europeans' privacy and at the same time enabling innovation. Achieving this requires that we strike a careful balance. On the one hand, companies that process data must be transparent about their processing practices and be responsible and accountable for applying high standards of data protection. But at the same time, the EU Regulation should not dictate in a highly prescriptive way how privacy protections are to be implemented,

nor should it introduce new burdens on controllers and processors that ultimately do little to advance privacy.

Instead, organisations should be given flexibility to develop privacy protections that suit the circumstances involved, and should be given strong incentives to innovate to provide the strongest possible protections. And where organisations fail to adequately secure and protect the personal data in their care, they should face meaningful penalties.

The proposed Regulation takes important steps forward in this regard. For example, the proposal includes measures requiring that organisations design technologies with privacy in mind, are transparent about their processing activities, and remain responsible for how they use personal data. The proposal also helpfully addresses inconsistent rules and interpretations across the 27 EU Member States via, for example, the "one-stop-shop" approach.

However, other proposals need refining to ensure that the protections they offer are both strong *and* workable. For that reason, we think some amendments to the Regulation may be appropriate, among them in relation to:

- **International data transfers:** The Regulation introduces important new mechanisms to facilitate the secure flow of personal data, including in the cloud. These mechanisms include new rules on "standard" contractual clauses. We welcome these measures. But Microsoft also believes that cloud processors and others should be encouraged to go beyond the "baseline" safeguards set out in the Regulation in certain contexts. Where controllers and processors have practical experience that suggests that additional safeguards are appropriate to protect data, they should be incentivised to adopt these safeguards. Our amendments create a mechanism to do this. Specifically, our amendments:
    - propose a change to Article 42 to make it clear that organisations can offer supplemental, legally binding protections (e.g., data processing agreements) in addition to the protections included in the standard clauses,
    - propose a further change to Article 42 to offer organisations an incentive -- in the form of an EU data protection seal or trust mark -- to adopt such supplemental protections, and
    - propose a change to Article 39 (on certifications) that requires that any mechanisms for seals or trust marks are voluntary, affordable, technology neutral and capable of global recognition. This will ensure that certifications are open to the widest possible participation by all controllers and processors.
- **Processors and controllers**: Consistent with the existing EU framework, the proposed Regulation continues to allocate responsibilities between "data

controllers" and "data processors." Because controllers and processors have different obligations and liabilities, it is key that organisations understand when they are a controller and when they are a processor. The proposed Regulation would distinguish between these roles by defining "controllers" as those who are responsible for determining the "purposes, means and conditions" of processing. But with the evolution of new computing models, processors are playing a greater role in determining the means and conditions of processing. As a result, the line between controllers and processors is blurring. We propose an amendment that we believe will help to clarify what role a given entity is playing depending on their involvement in the processing of personal data. Specifically, our amendment would make it clear that the controller is the one who determines the *purposes* of processing.

- **One-stop-shop:** Today, companies that operate across Europe are subject to multiple and divergent national data protection regimes. To address this problem, the Regulation introduces a "one-stop-shop," based on the location of an organisation's "main establishment." This approach offers a significant improvement over the existing, fragmented regime. Less helpfully, however, the Regulation applies different tests for controllers and processors in determining their country of main establishment. As with the rules defining the terms "controller" and "processor," the approach to "main establishment" does not reflect how many organisations currently operate. Today, in practice, many controllers also act as processors. Proposing a test for main establishment that subjects controllers and processors to *different* tests means that those controllers that also act as processors will be once again subject to multiple national authorities, and will find themselves unable to benefit from the one-stop-shop. We propose an amendment that would subject controllers to the same test as processors when they are playing both roles.

- **Delegated acts:** The Regulation includes 26 provisions conferring power on the Commission to adopt delegated acts. These provisions should be significantly reduced. For example, many of these provisions deal with essential elements of the law. These essential elements should be addressed in the Regulation itself, not left to secondary law-making by the Commission. Other delegated act provisions give the Commission power to prescribe technical formats, standards and solutions -- threatening to replace industry innovation with regulatory intervention. Our proposed amendment would delete those provisions that relate to essential elements of the law and/or that are better addressed through innovation. Finally, as the Article 29 Working Party and the EU Data Protection Supervisor have noted, the delegated act provisions do not include a clear timetable for implementation. Our amendment would also introduce a deadline for the adoption of delegated acts.

- **Administrative fines/sanctions:** Data protection obligations are only effective to the extent they are enforced. Consistent with this view, the Regulation includes strong sanctions for violations. Less helpfully, however, the Regulation takes a "one-size-fits-all" approach, and could be read to apply the same sanctions to deliberate, flagrant violations of the rules as it does to violations that are merely accidental. This means that a company that

inadvertently fails to use a specific electronic format when giving a customer access to his information could face the same penalty as a company that repeatedly and intentionally collects and processes data about individuals without informing those individuals about its activities. To be balanced and effective, the Regulation should ensure that the most punitive sanctions are reserved for truly bad actors.

- **Data breach**: Requiring data controllers to notify serious data breaches to competent authorities and to data subjects will drive a higher standard of data security across industry. But any breach notice regime must be workable in practice. The proposed Regulation would compel controllers to give notice of non-serious breaches. This approach threatens to overwhelm DPAs and data subjects with notices about breaches that ultimately prove immaterial -- which in turn may lead data subjects ultimately to ignore notices. Our amendments seek to ensure that notice is required only where a breach is likely to lead to serious risk of significant harm to a data subject.

International Data Transfer/Standard Clauses

Amendment
Proposal for a regulation
Recital 83 a (new)

Text proposed by the Commission	*Amendment*
	(83a) In light of increasing cross-border flows of personal data, controllers and processors should be encouraged to offer robust safeguards for data subjects where personal data is transferred to third countries. Controllers and processors will often have pragmatic experience that demonstrates a need for additional, specific protections to reflect the particular circumstances or requirements of data subjects. In such cases, controllers and processors should be encouraged to adopt additional measures to supplement the safeguards for data transfer set out in the Regulation. Member States and supervisory authorities should recognise those controllers and processors that adopt such additional protections[, which may, for example, include supplemental, legally binding commitments that apply in addition to standard data protection clauses]. Such recognition may take the form of data

protection seals or marks at the European level.

Amendment
Proposal for a regulation
Article 42 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. A controller or processor may choose to base transfers on standard data protection clauses as referred to in points (b) and (c) of paragraph 2 of this Article, and to offer in addition to these standard clauses supplemental, legally binding commitments that apply to transferred data. In such cases, these additional commitments shall be subject to prior consultation with the competent supervisory authority and shall supplement and not contradict, directly or indirectly, the standard clauses. Member States, supervisory authorities and the Commission shall encourage the use of supplemental and legally binding commitments by offering a data protection seal, mark or mechanism, adopted pursuant to Article 39, to controllers and processors who adopt these heightened safeguards.

Justification

With the increasing globalisation of business and the evolution of computing models like the cloud, cross-border flows of personal data have become routine. In this environment, it is critical that controllers and processors apply strong safeguards to personal data regardless of where that data is located. Users will only have confidence in cloud computing if they know that their data is safe in the cloud.

Helpfully, the Regulation already requires that transfers of personal data to third countries may only be carried out in full compliance with the Regulation. This is an important principle. But controllers and processors should be incentivised to go beyond the Regulation in some cases. Indeed, controllers and processors will often have direct and practical experience that demonstrates that additional safeguards -- i.e., safeguards that supplement those in the Regulation -- may be appropriate in relation to the personal data they are transferring. The Regulation should encourage these controllers and processors to offer supplemental safeguards where these are appropriate.

The amendment proposed above would help to achieve this is by allowing controllers and processors that base data transfers on standard data protection clauses under Articles 42(2)(b) and 42(2)(c) of the Regulation to also offer additional protections to customers in the form of legally binding contractual commitments (e.g., data processing agreements) that expand on the standard clauses. In this way, controllers and processors can offer additional protections that reflect the ways in which they will be processing data and particular safeguards appropriate to that processing. Of course, these supplemental commitments should not contradict the standard clauses.

To encourage controllers and processors to adopt these heightened commitments, Member States and supervisory authorities should offer recognition in the form of a data protection seal or mark. These measures could be adopted pursuant to Article 39 of the Regulation. (We propose a corresponding amendment to Article 39 below.)

Amendment

Proposal for a regulation

Article 39 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the	1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly

level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.	assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall ***be voluntary, capable of global application and affordable. These mechanisms shall also be technology neutral and shall*** contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

Justification

As described above, a certification scheme may help to encourage organisations to provide additional safeguards -- beyond standard clauses -- to personal data transferred out of the Union. If the Parliament chooses to move forward with such a certification scheme, it should do so in a way that promotes the broadest possible participation. Indeed, any certification regime should be structured so as to avoid unduly burdening companies (particularly SMEs) with costly and bureaucratic obligations that discourage participation.

The amendment proposed above to Article 39 would introduce important conditions on certification schemes that would ensure they are widely usable by controllers and processors large and small. Specifically, certification schemes would need to:

- *Be voluntary. Mandatory certification schemes can chill innovation and deter competition in the development of enhanced privacy protections – just at a time when we are seeing an acceleration of innovation and competition in the privacy sphere.*
- *Be affordable. Some privacy certification regimes involve costs of upwards of €150,000 simply to certify one feature of a product or service. These costs create barriers to entry for all but the largest service providers, and discourage wide-scale use of the regime.*
- *Be capable of being rolled-out and recognised globally. To help reduce the compliance burden on providers, any certification scheme should be capable of being endorsed by regulators in third countries as well as by those in the Union.*
- *Be neutral as to system, service or technology. Similarly situated services and products should be subject to the same assessment criteria. Favouring some solutions over others creates market distortions and hinders innovation.*

Controllers/Processors

Amendment
Proposal for a regulation
Article 4 – point 5

Text proposed by the Commission	*Amendment*
(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes***, conditions and means*** of the processing of personal data; where the purposes***, conditions and means*** of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes of the processing of personal data; where the purposes of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

Amendment
Proposal for a regulation
Article 24

Text proposed by the Commission	*Amendment*
Where a controller determines the purposes***, conditions and means*** of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.	Where a controller determines the purposes of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

Justification

The EU's data protection framework distinguishes between "data controllers" and "data processors," with both groups subject to different obligations. The proposed Regulation also follows this controller/processor structure to a degree. As a result, in order for organisations to understand fully their obligations under the Regulation, they need to know when they are operating as controllers and when they are operating as processors.

Today, however, there is increasing confusion about the distinction between the two roles. The test proposed under the Regulation will not improve this situation. Under the test proposed in the Regulation, controllers are deemed to be those organisations that make decisions about the "purposes, means and conditions" of processing data. But as processors become more sophisticated and play a greater role in supplying the "means" and determining the "conditions" of processing, the lines between controllers

and processors are beginning to blur. We anticipate that these lines will continue to blur moving forward.

The above amendment would redefine the term "data controller" as the entity that determines the "purposes" of the processing. This change recognises that controllers and processors today often have some degree of shared responsibility with regard to supplying the means and deciding the conditions of processing. It also recognises that this shared responsibility should not be determinative for deciding when an organisation is a controller. This change will help to clarify the divide between the important roles of controller and processor and create greater legal certainty.

This amendment would also make corresponding changes to Articles 24 (on "Joint Controllers") to reflect the change to the definition in Article 4.

Amendment
Proposal for a regulation
Article 26 – paragraph 5

Text proposed by the Commission	*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 for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.	***deleted***

Justification

The Lisbon Treaty makes clear that delegated acts are meant to be used to "supplement or amend certain non-essential elements" of a law. In the context of the proposed Regulation, however, the Commission often appears to be using delegated acts to determine the scope and applicability of core aspects of the law -- including with regard to fundamental issues such as the obligations of processors (Article 26(5)).

The obligations of processors should be clearly defined in the Regulation itself. Europe's processors -- and the controllers and data subjects they serve -- should not be required to wait for secondary legislation to be adopted in order to understand the responsibilities, duties and tasks that apply to processors. For this reason, Article 26(5) should be deleted.

One-Stop-Shop / “Main Establishment”

Amendment
Proposal for a regulation
Article 4 – point 13

Text proposed by the Commission	*Amendment*
(13) ‘main establishment’ means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;	(13) ‘main establishment’ means as regards the controller, ***including a controller that is also a processor,*** the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor ***that is not also a controller,*** 'main establishment' means the place of its central administration in the Union;

Amendment
Proposal for a regulation
Recital 27

Text proposed by the Commission	*Amendment*
(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of	(27) The main establishment of a controller in the Union, ***including a controller that is also a processor,*** should be determined according to

management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.	objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor ***that is not also a controller*** should be the place of its central administration in the Union.

Justification

Today, enterprises operating across the Union find themselves required to comply with multiple and often diverging national data protection regimes. This situation creates legal uncertainty and impedes the free flow of data in the Union.

The proposed Regulation seeks to improve this situation by subjecting enterprises that are processing data in the Union to a single law and a single supervisory authority in the country of "main establishment" (the so-called "one-stop-shop"). This is a significant step forward. Greater harmonisation will dramatically reduce the compliance burdens on European organisations while at the same time ensuring a high level of protection for data subjects.

Less helpfully, however, in determining the location of an organisation's "main establishment," the Regulation applies a different test for controllers and processors. This approach ignores the fact that some controllers are

also processors. In these cases, it makes little sense to apply different tests. Doing so will result in these controllers once again faced with the need to comply with multiple regimes.

The amendment above takes a more sensible approach, and applies the same test to controllers and processors in those cases where the controller is also acting as a processor. This approach ensures that such controllers are fully able to benefit from the one-stop-shop that is the centrepiece of the proposed Regulation.

Delegated Acts

Amendment
Proposal for a regulation
Article 86 – paragraph 2

Text proposed by the Commission	*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(7),***[1] 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 12(5), Article 14(7), Article 15(3), Article 20(6), Article 23(3), Article 28(5), Article 35(11), Article 37(2), Article 39(2), 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.

Amendment
Proposal for a regulation
Article 86 – paragraph 3

Text proposed by the Commission	*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),	3. The delegation of power referred to in Article 12(5), Article 14(7), Article 15(3), Article 20(6), Article 23(3), Article 28(5), Article 35(11), Article 37(2), Article 39(2), 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 revocation shall

1 *Note that this Article is mis-cited in the proposed Regulation as Article 79(6). The correct reference is to Article 79(7).*

Article 43(3), Article 44(7), Article 79(7), 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 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.

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.

Amendment
Proposal for a regulation
Article 86 – paragraph 4

Text proposed by the Commission	*Amendment*
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	4. ***The Commission shall present proposals for delegated acts to be adopted pursuant to Article 12(5), Article 14(7), Article 15(3), Article 20(6), Article 23(3), Article 28(5), Article 35(11), Article 37(2), Article 39(2), Article 81(3), Article 82(3) and Article 83(3) within two years of the date of publication of this Regulation in the Official Journal of the European Union.*** As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

Amendment
Proposal for a regulation
Article 86 – paragraph 5

Text proposed by the Commission	*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(7),*** 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 12(5), Article 14(7), Article 15(3), Article 20(6), Article 23(3), Article 28(5), Article 35(11), Article 37(2), Article 39(2), 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

Of the 91 articles in the Regulation, 26 include provisions that would allow the Commission to adopt "delegated acts." Each delegated act provision empowers the Commission to create new, secondary legal regimes, binding across the EU.

The many delegated act provisions mean that organisations could face new rules for many years after the Regulation is adopted. This creates confusion about data subjects' rights. It also makes it difficult for organisations

processing data to understand their obligations. Because the Regulation includes substantial sanctions for non-compliance (up to 2% of annual worldwide turnover for certain violations), it is critical that organisations understand clearly what their obligations are.

To address these issues, the number of delegated acts should be significantly reduced. Delegated acts should be used only where needed and appropriate. Specifically:

1. ***Consistent with the Lisbon Treaty, any delegated act provisions that deal with essential elements of the law should be deleted.*** *Many of the delegated act provisions -- including Article 6(5), Article 9(3), Article 22(4), Article 26(5), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 43(3), Article 44(7) and Article 79(7) -- address essential elements of the data protection framework. However, under the Lisbon Treaty, delegated acts are intended to supplement "non-essential elements" of the Law. Essential issues should be addressed in the Regulation, not deferred until a later date. Allowing the Commission to defer legislating on essential elements of the law undermines legal certainty and makes it difficult for companies to plan for compliance. These Articles should be deleted.*

2. ***Consistent with EU policy, those delegated acts that allow the Commission to dictate how technologies should be developed should also be deleted.*** *Certain delegated acts provisions -- including Article 8(3), Article 17(9) and Article 30(3) -- threaten to undermine the principle of technology neutrality by allowing the Commission to adopt prescriptive rules, standards and formats. Technology neutrality is well established in European law and policy. Technology neutral policies allow for competition among different solutions, which in turn drives innovation. At the same time, technology neutrality ensures that legislation is not "frozen in time," as technology evolves. But by allowing the Commission to dictate how obligations should be implemented at a technical level, these provisions give the Commission the power to substitute regulatory intervention for industry innovation. Again, these Articles should be deleted.*

3. ***Delegated acts that remain in the Regulation should be subject to a clear timetable for adoption.*** *Without a clear timeline for the adoption of delegated acts, controllers, processors and data subjects could face a lengthy period of uncertainty about their obligations and their rights. The Article 29 Working Party has acknowledged this concern, stating in its Opinion on the proposal that "At the very least the Working Party calls on the Commission to set out which delegated acts it intends to adopt in the short, medium and long term."*

[Corresponding amendments will need to be made to Recital 129 and Recital 131 and Article 6(5), Article 8(3), Article 9(3), Article 17(9), Article 22(4), Article 26(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 43(3), Article 44(7), and Article 79(7).]

Administrative Sanctions

Amendment
Proposal for a regulation
Article 79

Text proposed by the Commission	*Amendment*
1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.	1. Each ***competent*** supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.
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 co-operation with the supervisory authority in order to remedy the breach and the degree of co-operation with the supervisory authority in order to remedy the breach	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 sensitivity of the data in issue,*** the intentional or negligent character of the infringement, ***the degree of harm or risk of significant harm created by the violation,*** 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 co-operation with the supervisory authority in order to remedy the breach. ***In setting an administrative fine, supervisory authorities shall also take into account fines, damages or other penalties previously imposed by a court or other body on the natural***

or legal person in respect of the violation in issue.

2a. Aggravating factors that support administrative fines at the upper limits established in paragraphs 4 to 6 shall include in particular:

(i) repeated violations committed in reckless disregard of applicable law,

(ii) refusal to co-operate with or obstruction of an enforcement process, and

(iii) violations that are deliberate, serious and likely to cause substantial damage.

2b. Mitigating factors which support administrative fines at the lower limits shall include

(i) measures having been taken by the natural or legal person to ensure compliance with relevant obligations,

(ii) genuine uncertainty as to whether the activity constituted a violation of the relevant obligations,

(iii) immediate termination of the violation upon knowledge, and

(iv) co-operation with any enforcement processes.

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.	
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***:	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.
....	
	4. The supervisory authority ***may, in its discretion,*** impose a ***total*** fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover ***up to a maximum of 500 000 EUR per case***, to anyone who, ***in deliberate violation of law or with reckless disregard for applicable obligations***:
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****:*	
. . . .	
	. . . .
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***:	5. The supervisory authority ***may, in its discretion,*** impose a ***total*** fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, ***up to a maximum of 1 000 000 EUR per case***, to anyone who, ***in deliberate violation of law or with reckless disregard for applicable obligations***:
. . . .	
	. . . .
The Commission shall be empowered to adopt delegated acts in accordance with	6. The supervisory authority ***may, in its discretion,***

Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.	impose a ***total*** fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover ***up to a maximum of 2 000 000 EUR per case***, to anyone who, ***in deliberate violation of law or with reckless disregard for applicable obligations***: . . . . ***Where evidence exists to demonstrate the continued failure of the sanctions established in paragraphs 1 to 6 of this Article to address serious abuses, t***he Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.

Justification

These amendments modify the proposal in four key ways:

- *First, the amendments specify the mitigating and aggravating factors that supervisory authorities should consider when imposing fines. In doing so, the amendments ensure that higher fines are imposed on more serious misconduct, and also encourage compliance and co-operation once a violation is discovered. Specifying these factors will also promote greater consistency across the Member States in terms of the fines imposed.*

- *Second, on the role that the Supervisory Authority will play, the amendment proposes to replace the term "shall" by "may in its discretion". This is to avoid burdensome and bureaucratic procedures for minor infringements and to emphasise the fact that there are circumstances where such administrative fines would be disproportionate. It is up the independence and discretion to the Supervisory Authority to decide how to use this sanction.*

- *Third, the amendments make clear that where an individual or entity has already been subject to sanction in another proceeding (such as a civil judgment), that fact should be considered in assessing a fine. This avoids penalising a party twice for the same conduct.*

- *Finally, the amendments reflect the fact that while deliberate or reckless violations of the proposed Regulation should merit substantial penalties, imposing the same penalties on merely negligent violations would be disproportionate. The proposed amendments allow supervisory authorities to impose administrative fines that constitute meaningful deterrents; at the same time, these provisions ensure that the most punitive sanctions are reserved for truly bad actors.*

If the Commission nonetheless concludes that negligent conduct should also be covered in the Regulation, it is crucial to specify the language on how negligence should be assessed. We would recommend the following:

1. *The supervisory authority may also impose administrative sanctions in the case of negligent violations of the provisions identified in paragraphs 4, 5 and 6. In cases of negligent violation, the administrative fine shall be set at the lower limit of the ranges established in paragraphs 4, 5 and 6, and shall take into account the criteria referred to in paragraphs 2, 2(a) and 2(b).*

2. *Negligent violations are those where the natural or legal person:*
   - *(i) fails to take appropriate measures to ensure that the processing of personal data is performed in compliance with its obligations;*
   - *(ii) does not commit the violation deliberately or with reckless disregard of the relevant obligations; and*
   - *(iii) in committing the violation, exposes the data subject(s) to substantial risk of harm.*

Data Breach

Amendment
Proposal for a regulation
Article 31 – paragraph 1

Text proposed by the Commission	*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 ***that is likely to lead to significant risk of substantial harm to a data subject***, the controller shall without undue delay notify the personal data breach to ***its competent*** supervisory authority.

Amendment
Proposal for a regulation
Article 31 a (new)

Text proposed by the Commission	*Amendment*
	Notification of a personal data breach shall not be required if the controller demonstrates to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Amendment
Proposal for a regulation
Article 31 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission shall be	***deleted***

empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

Amendment
Proposal for a regulation
Article 32 – paragraph 1

Text proposed by the Commission	*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. ***Upon determination by the competent supervisory authority,*** when the personal data breach is likely to ***lead to significant risk of substantial harm to*** 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.

Amendment
Proposal for a regulation
Article 32 – paragraph 5

Text proposed by the Commission	*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

Breach notice obligations provide important incentives to data controllers to be responsible in their management of data, and will help to drive a higher standard of data security across industry. Requiring notice of breaches also fosters confidence of data subjects in third party processing.

To be effective, the breach notice regime must be practical and workable. The regime should not overly burden DPAs nor should it require that controllers notify breaches that prove harmless, which could lead data subjects to suffer from "notification fatigue". To achieve these ends, the amendments above make three important changes to the proposed Regulation:

- ***First, the amendments would eliminate the obligation to notify within 24 hours.*** *There is significant consensus among industry and regulators that notice within 24 hours is not feasible. Controllers need more time to understand the nature of the breach, who is affected, and whether the breach poses harm to the data subjects involved.*

- ***Second, the amendments make clear that notice is required only where the breach threatens significant risk of serious harm to the data subject.*** *Requiring notifications only where serious harm is threatened reduces the likelihood that data controllers issue immaterial notices that may lead, over time, to consumers ignoring them. This requirement also reduces the burden on DPAs, which would otherwise be obligated to spend time and resources investigating harmless breaches. For this same reason, the amendments make clear that no notification is required where data has been rendered unintelligible through the application of technological protection measures.*

- ***Finally, the amendments delete references to delegated acts.*** *Given the essential nature of breach obligations to the Union's data protection framework, the rules on breach should be addressed in the Regulation itself -- and not left to secondary rulemaking.*

Note that corresponding amendments will be required to Recital 67.