Microsoft
Microsoft
Corporate Affairs Europe | Tel +32 (0) 2 704 39 10
Avenue de Nerviens 85 | B-1040 Brussels

For more information, please contact Jean Gonié, Director of Privacy EMEA Policy,
or Tanja Böhm, Manager Government Affairs, tanja.boehm@microsoft.com
or Jörg-Alexander Albrecht, Manager Government Affairs, a-joalb@microsoft.com

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

Microsoft positions at a glance

Microsoft welcomes the draft Data Protection Regulation. As a company committed to user privacy, we believe in being transparent with our customers about our data protection practices and we work had to develop innovations that empower our customers to exercise choice and control over their personal information. Our commitment is exemplified throughout our products and services, including in our decision to turn on the Do Not Track signal in Internet Explorer 10, and in our Office 365 Trust Center, which gives users of our cloud services detailed information about our privacy policies and practices.

We believe that industry and consumers can benefit from clear, harmonised data protection rules. But we also recognise that online companies in particular need some flexibility to innovate and to develop new privacy solutions. Our proposed amendments seek to strike this balance -- requiring organisations to commit to strong protections and to be transparent and accountable while balancing the many benefits that today's technology can provide. Specifically, we propose:

1/ Rules that promote secure data transfers in the Cloud (p. 5). *Our first amendment would encourage good practices by rewarding organisations that demonstrate responsibility by applying the appropriate protections to data they transfer outside of the Union, including in relation to the transfer of data in the Cloud. We also propose an amendment to extend and standardise the EU's robust protections on data transfers to sub-processors, who play an increasingly important role in the Cloud.*

2/ Clearer rules for controllers and processors (p. 12). *Under the proposed Regulation, controllers and processors are subject to different obligations. We propose a clear test that organisations can apply to determine their status (i.e. controller or processor) and pinpoint which supervisory authority has jurisdiction over them.*

3/ More effective breach notices (p. 17). *Breach notice will drive improved data security and transparency across industry. Our amendment would ensure that breach notice rules are crafted in a way that makes sure data subjects pay close attention to notices that matter to their data protection interests.*

4/ Meaningful but proportionate penalties (p. 19). *Administrative fines are an essential part of the new regime. But the Regulation's "one-size-fits-all" approach treats companies that intentionally cause harm exactly the same way as it treats negligent companies. This is disproportionate. Our amendment empowers DPAs to impose out strong, but fair penalties.*

5/ Delegated acts only where necessary (p. 23). *The sheer number of delegated acts threaten to create significant business and consumer uncertainty. Our amendment would reduce the number of delegated acts.*

***

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:

1. **International data transfers.** The Regulation introduces important mechanisms to facilitate the secure flow of personal data, including in the cloud. These mechanisms include "standard contractual clauses" ("SCCs"). SCCs, which require organisations to apply certain baseline protections to transferred data, are used routinely today to transfer data outside of the Union. Microsoft strongly supports SCCs, and we offer these to our enterprise cloud customers. But we also believe that **cloud processors and others should be encouraged to go *beyond* the baseline safeguards in the SCCs in certain situations**.

   Our amendments create a mechanism to do this. Specifically, our amendments propose a change to Article 42 to offer organisations an *incentive* -- in the form of an EU data protection seal or trust mark -- to adopt supplemental protections for transferred data. And we also propose a change to Article 39 (on certifications) that requires that any mechanisms for seals or trust marks are voluntary, affordable, technology neutral, transparent and capable of global recognition. This will ensure that certifications are open to the widest possible participation by all controllers and processors.

We also propose an amendment that would **extend standard contractual clauses to sub-processors**, as recommended on pages 74 and 80 of a Parliament Policy Department study prepared for the IMCO Committee, "Reforming the Data Protection Package"[1] (the "Parliament Study"). Today, cloud providers often rely on sub-processors. Extending SCCs to sub-processors means that EU-based cloud providers will have greater flexibility in choosing sub-processors, and that consumers can be confident their transferred data is secure. This approach echoes the recommendations in the Parliament Study. It is also consistent with the recommendation in the Article 29 Working Party's Opinion 05/2012 on Cloud Computing, where the WP suggested that "a written agreement which imposes the same obligations on the sub-processor as are imposed on the processor in the [SCCs] should be put in place".

2. **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 operating as a controller and when they are a processor. **Our amendments make the line between controllers and processors clearer**: when an organisation determines why personal data is processed (i.e. for what purposes), that organisation is a controller. When an organisation only determines how personal data is processed (i.e. the means and conditions of the processing), that organisation is a processor. This approach is consistent with a recommendation made in the Parliament Study[2].

   Our proposed amendments would also **make it easier for organisations to determine the location of their "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." But the Regulation applies different tests for controllers and processors when 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. We propose an amendment that would subject controllers to the same test as processors when they are playing both roles.

3. **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. It does not make sense, for example, to treat the case where an online computer gaming account is hacked and the hacker gains access to a player's gaming achievements

[1] "Reforming the Data Protection Package" Study, pg. 74, 80 - Directorate-General for Internal Policies, Policy Department, Economic and Scientific Policy, Internal Market and Consumer Protection, available at http://www.europarl.europa.eu/document/activities/cont/201209/20120928ATT52488/20120928ATT52488EN.pdf

[2] Idem, pg. 31, 41.

in the same way as a breach of a patient's electronic medical records. 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.

4. **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, for example, 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.

5. **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.

International Data Transfer/Cloud

Amendment
Proposal for a regulation
Recital 84

Text proposed by the Commission	*Amendment*
(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.	(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. ***In some scenarios, it may be appropriate to encourage controllers and processors to provide even more robust safeguards via additional contractual commitments that supplement standard data protection clauses.***

Amendment
Proposal for a regulation
Article 42 – paragraph 2 e (new)

Text proposed by the Commission	*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) contractual clauses between the controller or processor and the recipient of the data that supplement standard data protection clauses as referred to in points (b) and (c) of paragraph 2 of this Article, and are authorised by the competent supervisory authority in accordance with paragraph 4.***

Amendment
Proposal for a regulation
Article 42 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.	4. Where a transfer is based on contractual clauses as referred to in point (d) ***or (e)*** of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the ***competent*** supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the ***competent*** supervisory authority shall apply the consistency mechanism referred to in Article 57***.***

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

Text proposed by the Commission	*Amendment*
	4a***. To encourage the use of supplemental contractual clauses as referred to in point (e) of paragraph 2 of this Article, competent authorities may offer a data protection seal, mark or mechanism, adopted pursuant to Article 39, to controllers and processors who adopt these safeguards.***

Justification

This amendment encourages data controllers and processors to apply the strongest protections possible to data they transfer outside of the Union.

Companies routinely now need to transfer personal data out of the Union to third countries for processing. The current Directive (95/46) generally prohibits transfers of data outside of the Union,

however, unless the receiving country has been deemed by the Commission to offer "an adequate level" of data protection. Where a country has not been deemed "adequate", a company can only transfer data if it can rely on an exception in the Directive, such as using "standard contractual clauses" that the Commission or national DPAs have approved.

Standard clauses are widely used today by organisations that transfer data. Effectively, they impose a legally binding obligation on organisations outside of the Union to apply certain "baseline" protections to data that has been transferred from the Union, including requirements to implement adequate security measures to protect data. The clauses also regulate liability for any damages suffered by individuals between the companies that export and import the data, and enable individuals whose data has been transferred to enforce certain provisions.

We believe that these baseline protections should be viewed as a minimum. In many cases, it may be appropriate for organisations to apply additional safeguards to protect data being transferred out of Europe -- i.e. to supplement the standard clauses with even more robust protections. The amendment above makes clear that organisations can do this, and also creates an incentive to adopt these supplemental protections in the form of a data protection seal or trust mark, which would foster innovation in privacy.

Specifically, the amendment proposed above would do two things:

(1) make clear that controllers and processors may supplement standard contractual clauses under Articles 42(2)(b) and 42(2)(c) of the Regulation with additional contractual commitments, thereby offering stronger protections to customers; and

(2) encourage controllers and processors to adopt these heightened commitments by offering them a data protection "seal of approval". The seal or trust mark 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 and paragraph 1 a (new)

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 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.	1. The Member States and the Commission shall ***work with controllers, processors and other stakeholders to*** encourage at European level the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors.
	1a. The data protection certifications

mechanisms shall ***be voluntary, affordable, and available via a process that is transparent and not unduly burdensome. These mechanisms shall also be technology neutral and capable of global application 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 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 **developed with stakeholder input at EU level**. To help create effective schemes and encourage widespread adoption, Member States and the Commission should work with stakeholders to establish the process of developing EU level certifications, seals and marks.*
- *Be **voluntary**. Mandatory certification schemes can chill innovation and deter competition in the development of enhanced privacy protections.*
- *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 available via a process that is **transparent and not unduly burdensome**. To ensure organisations apply for and adopt certifications, seals and marks that give individuals confidence about how their data is being processed, the process to apply for and be awarded a mark should not be unduly bureaucratic or burdensome.*
- *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.*

International Data Transfer/Subprocessors

I. Subprocessors: Definition

Amendment
Proposal for a regulation
Article 4, paragraph (6a)

Text proposed by the Commission	*Amendment*
	'subprocessor' means the processor processing personal data on behalf of another processor or subprocessor.

Justification

Data processors often subcontract processing activities to other companies, and such arrangements are now routine in the context of cloud computing. In order to ensure that these "subprocessors" are encompassed within the EU's data protection regime, these entities should be explicitly referenced in the Regulation -- including through a definition that clearly distinguishes the subprocessor from the original data processor and the data controller.

II. Subprocessors: Obligations

Amendment
Proposal for a regulation
Article 26, paragraph (2)

Text proposed by the Commission	*Amendment*
(d) enlist another processor only with prior permission of the controller;	(d) enlist a ***subprocessor*** only with prior permission of the controller;

Amendment
Proposal for a regulation
Article 26, paragraph (4a)

Text proposed by the Commission	*Amendment*
	Paragraph 2 shall not apply where a processing operation is carried out by a

	subprocessor and the processing is governed by a contract or other legal act binding the subprocessor to the processor [and stipulating in particular that the subprocessor will be subject to the same obligations as those imposed by the controller on the processor pursuant to paragraph 2, taking into account the role and processing activities performed by the subprocessor.]

Justification

Article 26(2)(d) of the proposed Regulation anticipates that a processor may use the services of a subprocessor. In these situations, the processor should enter into a legally binding agreement with the subprocessor. Such an agreement is important to ensure that the obligations that the controller imposes on the processor "flow down" to the subprocessor.

To that end, any contractual agreement between a processor and subprocessor should impose on the subprocessor the same obligations as those that the data controller imposed on the data processor, to the extent that those obligations are relevant in light of the activities performed by the subprocessor. This approach will help to protect controllers and data subjects, by ensuring that the subprocessor is fully obligated to protect the data entrusted to it.

III. Subprocessors: Standard Contractual Clauses

Amendment
Proposal for a regulation
Recital 84

Text proposed by the Commission	*Amendment*
(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.	(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers ***and*** processors ***and processors and subprocessors*** to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. ***In***

	some scenarios, it may be appropriate to encourage controllers and processors to provide even more robust safeguards via additional contractual commitments that supplement standard data protection clauses.

Amendment
Proposal for a regulation
Article 42 – paragraph 2(d)

Text proposed by the Commission	*Amendment*
2. (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.	2. (d) contractual clauses between the controller or processor and the recipient of the data***, which can be a subprocessor,*** authorised by a supervisory authority in accordance with paragraph 4.

Justification

In its Study on "Reforming the Data Protection Package", the Parliament's Policy Department points out that under the proposed Regulation, standard clauses do not extend to agreements between processors and sub-processors. As the Study points out, this gap could significantly disadvantage European firms, including new technology start-ups. The Article 29 Working Party has also recognised the need for sub-processors to be subject to the same obligations as apply to processors with regard to transferred data.

The amendment above is designed to close this gap. Without standard clauses -- a key tool enabling international data transfers -- European enterprises will be placed at a competitive disadvantage as they will restricted from choosing sub-processors outside of Europe.

For example, a European cloud start-up (the data processor) may build the service it offers to customers on technology offered by a third party (the sub-processor). Without standard clauses to protect the flow of data to sub-processors outside of the Union, the cloud start-up will be restricted in its choosing platforms on which to build its service -- and may, as a result, ultimately be forced to offer a cloud service that is less competitive.

In line with the Study's recommendation, the amendments above explicitly allow the Commission and Member States to extend standard clauses to sub-processors. This will give EU-based cloud providers and others greater flexibility and freedom in choosing adequate sub-processors.

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

Under the proposed Regulation, data "controllers" and data "processors" are subject to different obligations. In light of this framework, it is important that the Regulation include a clear test that organisations can apply to determine when they are operating as controllers and when they are operating as processors. The amendment above would introduce such a clear test.

*As a general rule, controllers typically determine **why** data is processed (i.e. for what purposes) while processors typically determine **how** it is processed (i.e. under what conditions). In a scenario where a cloud service provider offers enterprise customers a hosted email service, for example, the provider is likely to be a data processor. That's because the cloud service provider only determines "how" the data is processed -- i.e. it stores and delivers email for the purposes and at the direction of its enterprise customers. However, if the cloud service provider also uses the email addresses it collects from the service to profile end users and send them spam, then the cloud service provider has a say in the "why" the data is processed and becomes a data controller. In this scenario, the cloud service provider will be a controller for the same data for which it is a data processor.*

Unhelpfully, however, the test proposed under the Regulation confuses the simple "how" and "why" distinction -- making it harder for organisations to determine whether they are a controller or a processor or both. Under the Regulation, controllers are defined as those that determine not only the "purposes" of processing data (i.e. the "why"), but also the "conditions and means" of processing (i.e. the "how"). As the European Parliament's study has concluded, this approach isn't clear.

The above amendment would address this confusion by deleting the reference to "conditions and means," and making clear that the data controller is the entity that determines the "purposes" of the processing only -- i.e. the entity that determines the "why" data is processed. 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 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.	(27) The main establishment of a controller in the Union, ***including a controller that is also a processor,*** should be determined according to 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

The main establishment of the processor should be the place of its central administration in the Union.	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 potentially have to deal with 27 national regulators. The proposed Regulation improves this significantly by ensuring that enterprises that process data in the Union are regulated by a single supervisory authority in the country of "main establishment" (the so-called "one-stop-shop"). As the European Parliament has recognised, this is an important step toward a true Single Market for personal data that "reduces costs, ensures unity of application and increases legal certainty".

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. (For example, a cloud service provider may offer its customers a hosted e-mail service, but may also use the e-mail addresses it collects to provide its own services; in this scenario, the cloud service provider will be a controller for the same data for which it is a data processor.) In these cases, it makes little sense to apply different tests to determine which regulator has authority over the organisation. Doing so will result in these organisations being faced once again with having to deal with multiple regulators in different Member States.

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.

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 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.

Justification

These amendments would require controllers to notify only in the case of serious breaches. Notifying harmless breaches could have unintended effects: to begin with, it is likely to cause unwarranted anxiety among data subjects, but ultimately may lead to data subjects ignoring all notices. A requirement to notify harmless breaches would also burden data controllers and DPAs unnecessarily, leading to increased costs for European businesses. In order to ensure a healthy and trustworthy online environment, data breaches should be treated appropriately based on the likelihood of harm resulting from the breach. It does not make sense to treat a minor breach that threatens little or no damage to an individual -- for example, where an online computer gaming account is hacked and a hacker gains access to a player's game achievements -- the same way as a breach that is likely to create a significant risk of substantial harm, such as a breach involving sensitive personal data (e.g., an electronic medical record).

The proposed amendment to Article 31 also eliminates the obligation to notify within 24 hours, which industry and regulators alike recognize 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.

Note that corresponding amendments will be required to Recital 67.

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.

Justification

Notification of each and every breach, even where the breach does not threaten serious harm to individuals, would result in a system that is impractical, unreasonably expensive and unworkable. It also has a potential to create unwarranted anxiety among data subjects, and it can lead to significant cost increases for data controllers as well as DPAs. To help ensure that only serious breaches are notified, notification should not be required where data has been rendered unintelligible to those who obtain it, such as through the use of technological protection measures such as encryption, de-identification, etc.

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 established in paragraphs 4 to 6 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,
	(iv) co-operation with any enforcement processes, and
	(v) negligent violations characterised by a simple failure to act with due care, and not by intent.
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:***	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.
(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***: ….	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****:*	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***:
. . . .	. . . .
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, in its discretion,*** 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***:
. . . .	. . . .
The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.	***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

In order to create a healthy and secure online environment, companies must be held accountable when they fail to abide by the law. However, while deliberate or reckless violations of the proposed Regulation should merit substantial penalties, imposing the same penalties on merely negligent violations would be disproportionate and unfruitful. The Regulation currently treats deliberate and negligent breaches of the law exactly the same way, which is a flawed enforcement approach. The threshold of penalties for deliberate or reckless violations should certainly be higher than violations that result from negligence.

The above amendments, taken together, are designed to ensure that the penalty is proportionate to the conduct, and that the highest sanctions are reserved for the most serious misconduct.

Ensuring that supervisory authority has the full range of tools available to further the objectives of the regulation is critical to ensure the success of the Regulation. Therefore, the proposed amendments allow supervisory authorities the discretion to impose administrative fines that constitute meaningful deterrents -- but at the same time, they ensure that the most punitive sanctions are reserved for truly bad actors.

In addition, the amendments also clarify that only the competent Supervisory Authority should impose any fines. If multiple DPAs can sanction European businesses for the same violation, it would create a chilling effect on the business environment leading to reduced investment in technology related businesses. This amendment avoids organizations being sanctioned separately by 27 different DPAs for the same violation, which would undermine the Regulation's efforts to introduce a "one-stop shop" model.

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 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),***[3] 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 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) 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	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 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.

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

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 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 makes it difficult for organisations processing data to understand their obligations. It also creates confusion about data subjects' rights. Such regulatory uncertainly would negatively impact the internet economy in the European Union, especially for start-ups and growing businesses that particularly require regulatory consistency and stability in order to attract and sustain investment. Studies has shown that Small to Medium enterprises often are disproportionately affected by the cost of regulatory compliance.

While some delegated acts may be needed to clarify aspects of the Regulation, the Commission should adopt a strategy to carefully contain and manage the scope of such delegated acts. To address these issues, the number of delegated acts should be significantly reduced; where delegated acts are needed, the Regulation should specify the timeframe for adoption. 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 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.*

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 well-established Union principle of technology neutrality by allowing the Commission to adopt prescriptive rules, standards and formats. The pace of innovation in the technology industry is so rapid that any prescriptive rules on technical implementation are often outdated before they are even adopted. To avoid this scenario, the Commission should focus on "what", and allow the industry and market forces to determine "how".*

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).

Accountability obligations

Amendment
Proposal for a regulation
Article 22 - Responsibility of the controller

Text proposed by the Commission	*Amendment*
1.The controller shall ***adopt policies and*** implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	1. The controller, ***or the group of undertakings of which the controller is a member,*** shall implement appropriate measures to ensure and be able to demonstrate ***upon request*** that the processing of personal data is performed in compliance with this Regulation.
2. The measures provided for in paragraph 1 shall in particular include:	2. The measures provided for in paragraph 1 shall in particular include:
(a) keeping the documentation pursuant to Article 28;	***(a) management commitment and oversight to ensure processing of personal data is carried out in compliance with this Regulation, including, if appropriate, the appointment of the Data Protection Officer pursuant to Article 35.1;***
(b) implementing the data security requirements laid down in Article 30;	***(b) policies and procedures that document the requirements of this Regulation including the security requirements laid down in Article 30;***
(c) performing a data protection impact assessment pursuant to Article 33;	***(c) an assessment of risks associated with the processing of personal data such as, but not limited to, data protection impact assessments as required under Article 33;***
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	***(d) appropriate documentation of processing activities as laid out in Article 28;***
(e) designating a data protection officer pursuant to Article 35(1).	***(e) making appropriate summaries of its policies and procedures available to the relevant supervisory authority upon request, responding expeditiously to inquiries, complaints and requests from data subjects to access and where appropriate, to rectify, block or erase data the processing of which does not comply with the provisions of this***

legislation, in particular because of the incomplete or inaccurate nature of the data, and offering a recourse mechanism when harm occurs to a data subject due to a failure to comply with its policies and procedures; such measures shall be proportional to the nature and volume of the personal data that the controller processes, the nature of such processing, and the risks to the rights and freedoms of data subjects represented by such processing.

Justification

Consistent with the recommendations of the Article 29 Working Party (WP 173), this amendment introduces "accountability" into the regulatory framework. As recognised by the Working Party, accountability helps "move from theory to practice" by requiring data controllers and, via processing contracts, processors to adopt and implement meaningful, concrete measures to protect data – specifically, to put in place written policies and processes and controls to ensure such policies and processes are effectively implemented, to make appropriate summaries of those policies available to the responsible supervisory authority, to adopt appropriate security measures. Most global companies have global data privacy compliance programmes and these are set at global and group company level rather than for each controller. Moreover, the list of measures should be more flexible, listing what constitutes effective compliance without going into prescriptive detail on each of them. To be workable across the full spectrum of entities that handle data, the relevant obligations must be proportional and "scalable" – i.e., dependent on the nature of processing, the type of data, and the risks involved.