Telefónica's proposed amendments to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Directive)

Proposed Amendment 1

Article 4 Definitions	
Commission Proposal	Telefónica Amendment (proposed new text in blue)
For the purposes of this Regulation: (1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; (2) 'personal data' means any information relating to a data subject;	For the purposes of this Regulation: (1) 'personal data' means any data specifically relating to an identified living natural person or a natural person whose specific identity can be identified, directly or indirectly, by means likely reasonably to be used by the Controller; whilst identification number, location data, online identifiers, unique identifiers, or other specific factors as such can constitute personal data, they need not necessarily be considered as personal data in all circumstances, this will depend on the context. 2) 'data subject' means an identified living natural person or a living natural person whose specific identity can be identified, directly or indirectly, by means likely reasonably to be used by the Controller, in particular by reference to an identification number or other identifier(s) or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Justification:

The notion of what is and what is not personal data defines the scope of the regulation. Therefore, a clear definition is of outmost importance in order to ensure legal certainty.

Telefónica believes that the proposed definition of personal data is too broad: Personal data cannot simply be “any information relating to a data subject” (art.4.2). This would lead to too much information being deemed personal. Telefónica proposes a simpler definition.

The reference to a third party being able to identify an individual and this meaning that a controller possesses “personal data” means that under the proposed Regulation, a controller would have to live with a considerable amount of uncertainty. Data that is not considered “personal data” may transform itself into “personal data” if it is combined or cross-referenced with other data from a different source, or by some future technological innovation. The original data controller does not know what third parties or future technologies can do to make the data become “personal data”. This is a source of legal uncertainty.

Telefónica therefore believes that the definition should be reconsidered:

Firstly, Telefónica would like to emphasise that information should be “specifically” relating to the individual. This would seek to establish that even though information may relate to an individual e.g. be linked to an individual, it must be specifically about that individual. Hence “personal”. Hence aggregated data is not specifically about an individual.

Secondly, Telefónica seeks to make clear that you must be able to specifically identify the individual. In this way, anonymised data which does not reveal the identity of the individual to the recipient but which nonetheless uses a unique reference number would still be considered as providing “privacy” protection and hence not be considered personal data. For example, we want to ensure that where we release anonymous data to third parties, even though we (as a controller) may have the key to unlock the anonymisation, provided that the key is not provided to third parties, the data can still be considered anonymous.

Professional contact data and data related to deceased individuals should be excluded from the definition of personal data, as it already

occurs in the legislation of some Member States.

Telefónica welcomes the new wording "… by means likely reasonably to be used by the controller". Indeed, in some cases the means necessary to identify a natural person are not reasonable. In these cases, data should not be considered as personal. Furthermore, the means reasonably to be used should be in direct relation to the data controller. Therefore, Telefónica proposes that the reference to "or by any other natural or legal person" be deleted.

Finally, Recital 24 states: "identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances". Telefónica agrees with this, and for legal certainty and clarity, would suggest that this wording be introduced within the article itself and to also include "unique identifiers" to make clear that may not be personal data, provided that the key to unlock the anonymization is not provided to third parties.

Proposed Amendment 2

Article 4 Definitions	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(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~~, 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;

Justification:

The definition of controller should be based on the decision of the purposes for which personal data are processed (i.e. “why” the data are processed) rather than the conditions or means by which this is achieved (i.e. “how” the data are processed).

The control over the reason/purpose for processing is the logical basis for allocating different responsibilities between controllers who are responsible for what and why data is processed and processing parties who deal with how data is processed”.

A clear divide between controller and processor and their roles and responsibilities is key in a Cloud environment. More and more data processing is outsourced by the controller to a service provider (processor). Controllers often rely on their service providers to determine the most effective technological solutions to deliver outsourced processing. In fact, service providers sell themselves to their customers on the basis of their technical expertise, and necessarily exercise a certain, but limited, autonomy over the means and conditions by which they process data **on their customers’ behalf**. However, by doing so, service providers risk exposure under the current Proposal to the full compliance requirements of the Directive, a disproportionate burden when considering that the purposes for which they process data are entirely mandated by their customer as stated in the service agreement. It is also not in alignment with the typical practice of sharing responsibilities of the service providers and their customers in commercial agreements regarding such data processing services.

Proposed Amendment 3

Article 4 and Recital 25 Definitions	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed; Recital 25 "Consent should be given by any appropriate method enabling a freely given and informed indication of the data subject's wishes, either by a statement or by a clear action by the data subject, […] Silence should therefore normally not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided".	(8) 'the data subject's consent' means any freely given specific, informed and ~~explicit~~ unambiguous indication of his or her wishes by which the data subject, ~~either~~ for example by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed; Recital 25 "Consent should be given by any appropriate method enabling a freely given and informed indication of the data subject's wishes, either by a statement or by a clear action by the data subject, […] Silence should therefore normally not constitute consent, unless certain conditions providing information and control to the data subject are met. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided"

Justification:

In light of the existing case law and decision making practice, the term “explicit” is likely to be misunderstood to mean that data subjects are always required to tick a box, to state “yes, I accept my data to be processed”. This would lead to a very rigid regime incompatible with future services.

We propose that the word “explicit” be deleted and replaced with the term “informed, unambiguous consent”.

Indeed, requiring explicit consent combined with the requirement that the controller bears “the burden of proof for the data subject's consent to the processing of their personal data for specified purposes”, as provided for by Art. 7.1, is not workable especially in the digital environment and will hinder the development of innovative online services and products. Systematically requiring explicit consent may lead to practices which are both user unfriendly (“click fatigue”) while not leading to a higher level of privacy protection for data subjects.

User’s actions can provide a clear indication where there is a shared understanding of what is happening. For example, downloading a data based application on a mobile phone can constitute consent for the processing of personal data or other actions such as clicking an icon, sending an email or subscribing to a service.

In summary, the precise mechanisms by which valid informed consent is obtained may vary. The crucial consideration is that individuals must fully appreciate that they are consenting and what they are consenting to.

In addition, Article 6.1.b should be understood in a way that also covers those cases where a customer requires information based on his/her geographic location and is thus, by requiring the service, directly providing his/her authorization for personal location data to be processed.

Proposed Amendment 4

Article 4 Definitions of child	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(18) 'child' means any person below the age of 18 years;	(18)) 'child' means any person below the age ~~of 18~~ 13 years;

Justification:

We consider that the objective of this Regulation is to create consistent restrictions for the processing of personal data, wherever and however that processing occurs, and to provide clear protection for that data especially as it relates to children.

However, the definition of “child” in Art 4 point 18, creates two distinct age definitions in a single regulatory instrument, especially without clear definition or explanation regarding the requirements and circumstances applied to each age-group.

In the scope of a Regulation aimed exclusively at the processing of personal data, the creation of a distinction in online and offline data processing in the definition of a child seems an unnecessary, confusing, and potentially dangerous line to draw, only exacerbated by the definition-by-omission currently used to draw this distinction.

It is fundamental for an effective application of the new Regulation that definition of “child” in Article 4 be modified to set a single and clear restriction that does not allow the processing of personal data for anyone below the age of 13 years of age without parental authorization, regardless of the sector in which that processing occurs. In this sense, we suggest that a simple term in the customer contract whereby a parent “authorises” use of data relating to the device/account will be sufficient. Hence if they give the phone to a child, then they have authorised such use.

Finally, we would like to make a distinction between children and minors. A minor is any person below the age of 18. Pretending that minors in the upper range do not use online services means the regulation inapplicable. Therefore, we propose to consider a child that person below 13.

Proposed Amendment 5

Article 4 (New) **Definition of "anonymous data".**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
	(20) Anonymous data are those data altered in such a way that the specific identity of the data subject is no longer identifiable. To determine whether a person is specifically individually identifiable, account should be taken of all the means likely reasonably to be used by the controller (or by the recipient of the data in case of disclosures) to identify the specific individual.

Justification:

Telefónica fully supports the exclusion of "anonymous data" from the scope of this Directive.

However, the current Proposal is unclear and does not go far enough to give companies the guaranteed space to innovate and exploit new opportunities. Anonymization can allow organisations to publish or share useful information derived from personal data, whilst protecting the privacy rights of individuals.

Since "anonymous data" are the key to many future services, Telefónica firmly believes that a clear definition of anonymous data should be included in Article 4.

In this sense we propose a definition in which as long as the recipient is not reasonably likely to be able to identify the individual, then it is anonymous. In this way the controller can hold the key, and anonymous data can still be released provided that key is not provided to third parties. It is only if the controller releases the key -or the key is available- that the information should cease to be anonymous in the hands of the recipient.

Proposed Amendment 6

Article 6 Lawfulness of Processing	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of contract.	4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis in one of the grounds referred to in points (a) to (ef) of paragraph 1. This shall in particular apply to any change of terms and general conditions of contract.

Proposed Amendment 7

Article 7 Conditions for consent	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(4) Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	(4) ~~Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.~~

Justification:

Art. 7.4. is very broad and therefore does not provide the necessary legal certainty which is needed for a provision such decisive. Telefónica proposes its deletion.

Although, Recital 34 refers to the employment context, the current wording of Art.7.4. is too broad and could make this article applicable in all situations, even when a "good quality consent" had provided the legal basis for processing. Such wording leads to legal uncertainty.

An alternative to the above mentioned deletion it could be: “Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller, provided that the processing affects adversely to the data subject”

Proposed Amendment 8

Article 8 **Processing of personal data of a child**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.	For the purposes of this Regulation, ~~in relation to the offering of information society services directly to a child,~~ the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

Justification:

As the Regulation proposal currently stands, a “child” is defined as anyone under 18 years of age. However, the only mention of requirements that apply to a specific age-group is found in the new Article 8, entitled “Processing the personal data of a child”; the text of the Article refers only to requirements related to “a child below the age of 13 years” and to “information society services directly to a child”. This definition-by-omission leads to the conclusion that any service not considered part of the “information society” will be subject to different requirements for processing the data of a child (under 18 years of age); those services and/or their requirements, however, are not contemplated further in this Article or anywhere else in the current Regulation proposal.

Following this reasoning, Telefónica cannot find answers in the Regulation to some important questions related to processing the personal data of a child as What is the minimum age at which a data controller can process a data subject’s data offline (not included in “information society services”) or What differences exist in legal requirements or protection for children between the ages of 13 and 18, and to what specific activities or services are those differences applied?

We consider that the objective of this Regulation is to create consistent restrictions for the processing of personal data, wherever and however that processing occurs, and to provide clear protection for that data especially as it relates to children. In the scope of a Regulation aimed exclusively at the processing of personal data, the creation of a distinction in online and offline data processing in the definition of a child seems an unnecessary, confusing, and potentially dangerous line to draw, only exacerbated by the definition-by-omission currently used to draw this distinction.

Therefore it is fundamental for an effective application of the new Regulation that Article 8 on “Processing the personal data of a child” be modified to set a single and clear restriction that does not allow the processing of personal data for anyone below the age of 13 years of age without parental authorization, regardless of the sector in which that processing occurs.

Finally, we would like to make a distinction between children and minors. A minor is any person below the age of 18. Pretending that minors in the upper range do not use online services means the regulation inapplicable. Therefore, we propose to consider a child that person below 13.

Proposed Amendment 9

Article 10 **Processing not allowing identification**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	Data Protection Regulation should not apply to data rendered anonymous. If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.
Justification: Art. 10 provides that since some processing of data does not allow the controller to trace the data subject's identity, the controller itself will not be obliged to collect any further information in order to identify the data subject, even if so required by some provisions of the Regulation itself. But Article 10 should be clarified and improved as proposed above following the spirit of Recital 23.	

Proposed Amendment 10

Article 16 **Right of access**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed.	1. The data subject shall have the right to obtain from the controller ~~at any time~~, on request and under reasonable terms, confirmation as to whether or not personal data relating to the data subject are being processed.
Justification: Under some European Member States regulation, the right of access is a right that can be exercised only every twelve months, unless a legitimate interest is accredited. The reason why this right is temporarily limited is grounded in the fact that its exercise shall be free of charge. Therefore, we propose to limit this right of access when there are reasonable grounds to do it, i.e, when a legitimate interest is accredited.	

Proposed Amendment 11

Article 17 Right to be Forgotten	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(1) The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons.	(1) The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, ~~especially in relation to personal data which are made available by the data subject while he or she was a child,~~ where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons. new par. (2) The controller shall take all reasonable steps to communicate any erasure to each legal entity to whom the data have been disclosed, unless this involves

	a disproportionate effort.
(2) Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.	~~(2)~~ (3) Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform ~~third parties~~legal entities to whom the original controller had authorised to further process personal data ~~upon request of the data subject~~ and which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. In any case the controller will not be responsible for the personal data that the data subject by a voluntary act has made public.
(9) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying: (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	~~(9) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying: (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.~~

Justification:

The Right to be Forgotten is, in our view, not something new as data controllers already have to delete personal data whenever the data subject ask for erasure or cancellation. The basic principles on Data Quality (art. 6), Right of access and Right of rectification (Art. 12) and Consent (Art. 7) of Directive 95/46/EC are the basis of this "new right to be forgotten".

However, although we probably have a common understanding of what we want to achieve, the wording of the current proposal, especially of Art 17.2, extends the concept well beyond "personal data" and may oblige companies to delete data that is not personal in nature, such as information that someone has voluntarily published on the internet. Data controllers must inform any third party to "erase any links to, or copy or replication of that personal data". This information obligation is triggered by a request by the data subject to the original controller to erase data. This is technically far more challenging, if not impossible. This extended interpretation cannot and should not be the objective of this article.

With this extended scope of "personal data", this provision is difficult to apply in practice for social networking, blogs and Internet search businesses: the original controller of that data might not be aware of any third party processing. The controller would therefore have to track content across their service or worse across the entire Internet. In other words, by requiring that controllers inform any third parties, this provision seems to envisage that companies can oversee the entirety of the World Wide Web and control the information on it – an obligation that is directly at odds with the open architecture of the Internet. The e-Commerce Directive already recognises that it would be unreasonable to ask companies to monitor the Internet. It makes it clear that companies that act as intermediaries in the provision of services of the Information Society should not be required to do so.

In order to render this provision workable, we propose the following modifications:

This obligation should only be applied to personal data that the data subject has made available to the Data Controller specifically. Other data, for example, a journalist writing an article, tweets or someone commenting on a blog post, should be excluded from the scope of this obligation. Companies are only asked to "forget" personal data, not somebody's complete history. The data controller should not be responsible for the personal data that the data subject himself has made public.

The right to be forgotten should be limited to the original Data Controller who received the personal data directly from the user who contracted the service, and any third party who processes data on behalf of the Data Controller.

It should be clarified that no tracking of data published on own services is required from the controller and that the information obligation is only triggered by explicit request by the data subject and only to those third legal entities the controller directly authorised to further process personal data.

Telefónica welcomes the inclusion of Art. 13 on rights in relation to recipients, by which the obligation to inform is limited if it proves impossible or involves a disproportionate effort. Therefore, for the sake of legal certainty, Art. 13 should be moved in order to complete Art. 17.2. This would reinforce the wording related to "reasonable steps": "…the original controller shall take all reasonable steps, including technical measures, unless this proves impossible or involves a disproportionate effort".

Proposed Amendment 12

Article 18 **Right to data portability**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and [...]. 2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, [...]. 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, [...].	~~1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and [...].~~ ~~2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, [...].~~ ~~3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, [...].~~

Justification:

Data portability is fraught with technical and competition issues and therefore easier said than done. But apart from this enforcement difficulties, Telefónica would like to make a more important point: in essence, it is a competition or market organisation measure, but not related to data protection or privacy.

Transparency as a whole will be of further more importance to obtain confidence from our customers, therefore the market will provide for the most suitable forms of Data Subjects Access Rights. Some of our Operating Businesses are already today providing answers to customer requests for data in an electronic form and the customers are free to use it however they want. This will evolve in the future due to increasing amounts of data and the necessary process development going along with it.

We would, therefore, suggest striking it from this Regulation and strengthening and make easier the right to access to data. In other words to reinforce the data Subject Access Rights.

Proposed Amendment 13

Article 20 **~~Measures based on profiling~~ Automated Decision Making**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(1) Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.	(1) Every natural person shall have the right not to be subject to a ~~measure~~ decision which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to this natural person, ~~or to analyse or predict in particular the natural person's~~ such as his/her performance at work, ~~economic situation, location, health, personal preferences~~ creditworthiness, reliability or behaviour.
2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:	(2) Subject to other provisions of this Regulation, a person may be subjected to a ~~measure~~ decision of the kind referred to in paragraph 1 ~~only~~ if that decision:
(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been	(a) ~~is carried out~~ is taken in the course of the entering into, or performance of, a contract, ~~where~~ provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or ~~where~~ that there are suitable measures to safeguard his legitimate

adduced, such as the right to obtain human intervention; or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards. 3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9. 4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject. 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.	interests, such as arrangements allowing him to put his point of view; or (b) is ~~expressly~~ authorised by a Union or Member State law which also lays down measures to safeguard the data subject's legitimate interest; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards. ~~3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.~~ 4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a ~~measure~~decision of the kind referred to in paragraph 1~~ and the envisaged effects of such processing on the data subject.~~ ~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.~~

Justification:

The provisions on profiling are excessive and unclear, whilst we cannot see how they will enhance the user's privacy. There is a perception that profiling per se is bad. We would highlight that profiling can have very positive applications (eg.: traffic management).

Evenmore, Telefónica believes that "profiling" is not the main issue, but rather the consent is with automated decisions. The off and online world (both Private and Public Sectors) makes use of profiling day in day out in order to make decisions about what products, services, prices, levels of service, etc. are to be offered to customers. We understand that online behavioural advertising is singled out as a specific cause for concern which this Article seeks to regulate. In this sense we proposed to replace references to "profiling" and "measures" with "automated decision taking" in the recital and the article itself.

Article 20.4 obliges data controllers to ensure that data subjects are given sufficient information about the 'envisaged effects' of such processing on them. In addition, Article 33.2.a. obliges organisations to conduct Privacy Impact Assessments for such processing and to seek the views of the data subject or their representatives on it (Art. 33.4).

We call for the removal of this obligation to inform individuals about "envisaged effects" as it is an ambiguous and extremely subjective term and will be practically unworkable. The effects of a specific processing may be dependent on information and circumstances beyond the control of the data controller.

We are also calling for the removal of the obligations to conduct a Privacy Impact Assessment and to seek the views of data subjects or their representatives (Art. 33.2.a.). These requirements are excessive and costly and will not necessarily enhance the privacy of individuals.

Proposed Amendment 14

Article 25 **Representatives of controllers not established in the Union**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 2. This obligation shall not apply to: (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or (b) an enterprise employing fewer than 250 persons; or (c) a public authority or body; or (d) a controller offering only occasionally goods or services to data subjects residing in the Union. 3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside. 4. The designation of a	1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 2. This obligation shall not apply to: (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or ~~(b) an enterprise employing fewer than 250 persons; or~~ (c) a public authority or body; or (~~d) a controller offering only occasionally goods or services to data subjects residing in the Union.~~ 3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside. 4. The designation of a

representative by the controller shall be without prejudice to Legal actions which could be initiated against the controller itself.	representative by the controller shall be without prejudice to Legal actions which could be initiated against the controller itself.

Justification:

Article 25 (2) provides significant exceptions to this obligation in particular for enterprises employing less than 250 persons, public authorities or in the case of occasional offers of goods and services.

Telefónica does not understand why there should be an exemption from the obligation for enterprises employing less than 250 persons or in the case of occasional offers of goods and services. The simple fact that they are dealing with personal data of European citizens must be enough to be submitted to EU data protection rules. All European citizens deserve the same level of protection regardless of company size or assiduity in business relationship with customers resident in Europe.

We propose to delete point (b) and (d) from article 25 paragraph 2.

Proposed Amendment 15

Article 26 Processor	
Commission Proposal	Proposal (proposed new text in blue)
1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.	1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:	2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:
(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;	(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
(c) take all required measures pursuant to Article 30;	(c) take all required measures pursuant to Article 30;
(d) only enlist another further processors only with the prior permission of the controller that enable the requirements of this Regulation to be met;	~~(d) only enlist another further processors only with the prior permission of the controller that enable the requirements of this Regulation to be met;~~
(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;
(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;	(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;
(h) upon request make available to the controller and the supervisory authority all relevant and permissible information necessary to control compliance with the	(h) upon request make available to the controller ~~and the supervisory authority~~ all relevant and permissible information necessary to control compliance with the obligations laid

obligations laid down in this Article.	down in this Article.
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.	3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.
4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.	~~4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.~~
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.	~~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.~~

Justification:

This article introduces many new obligations on processors that should preferably be set in the contractual agreements between controllers and processors.

Furthermore, we suggest todelete the possibility for the Commission to adopt delegated.

Insofar we share the same thoughts than the Art. 29 Working Party reflected in its Opinion 8/2012 (October 5th, 2012, p. 26). We do not consider the relationship between a Controller and a Processor as "standardizeable" as various agreements are possible depending - for example - on the kind of data involved or the purposes of the processing. As far as the Controller according to Art. 26(1) has to take account of the general processing of personal data, we favour to leave space for individual agreements to generate an adequate protection level.

Proposed Amendment 16

Article 28 Documentation	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(1) Each controller and processor	(1) Each controller ~~and processor~~

and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility. 2. The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by thecontroller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; (g) a general indication of the time limits for erasure of the different categories of data; (h) the description of the	and, if any, the controller's representative, shall maintain documentation in respect of processing operations under its responsibility. 2. The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; c) a general description of its uses of personal data ~~(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);~~ ~~(d) a description of categories of data subjects and of the categories of personal data relating to them;~~ ~~(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;~~ ~~(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;~~ ~~(g) a general indication of the time limits for erasure of the different~~

mechanisms referred to in Article 22(3). 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 documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative. 6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	~~categories of data;~~ ~~(h) the description of the mechanisms referred to in Article 22(3).~~ ~~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 documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.~~ ~~6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Justification:

With the aim to reduce administrative burden on controllers, Art. 28 replaces the general obligation to notify individual processing operations to the supervisory authority under Articles 18(1) and 19 of Directive 95/46/EC. However, we believe this new obligation to maintain documentation of all processing operations will involve heavy bureaucratic requirements and therefore seriously risk increasing rather than reducing the administrative burden, compared to the current rules.

We are also concerned that identical obligations apply to data controllers and data processors (which currently are not subject to any notification obligation). This poses a particular problem in the area of cloud computing. Indeed, imposing disproportionate documentation obligations on data processors -identical to the controllers' obligations- risks severely slowing the development and roll out of new cloud computing offerings and services in Europe.

Finally, we firmly believe Article 28 conflicts with the principles of accountability and efficiency that are set out in Article 22 of the GDPR, therefore it should be simplified in order to become effective and proportionate. Only Article 28.2.a. and 28.2.b. should be maintained, combined with a general duty to keep an inventory and description of the way the controller ensures that processing operations comply with data protection rules.

Finally, we suggest to delete the possibility for the Commission to adopt delegated and implementing acts in line with Art.29 Working Party's Opinion 8/2012 (October 5th, 2012, p. 27).

Proposed Amendment 17

Article 30 **Security of processing**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(3) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.	~~(3) The Commission shall be empowered to adopt delegated acts in accordance with~~ ~~Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.~~
(4) The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to: (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	~~(4) The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:~~ ~~(a) prevent any unauthorised access to personal data;~~ ~~(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;~~ ~~(c) ensure the verification of the lawfulness of processing operations.~~ ~~Those implementing acts shall be adopted in accordance with the examination~~ ~~procedure referred to in Article 87(2).~~

Justification: We suggest to delete the possibility for the Commission to adopt delegated and implementing acts as the Commission does not know the technology and the architecture of companies. To meet the state of the art protection measures and to ensure the adequate and proportionate protection of personal data it is more appropriate to let companies build up the protection mechanism while implementing new products and services during the product development process itself.	

Proposed Amendment 18

Article 31 **Notification of a personal data breach to the supervisory authority**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(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. (2) Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach. (3) The notification referred to in paragraph 1 must at least: (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (c) recommend measures to mitigate the possible adverse effects of the personal	(1) In the case of a significant and material 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.~~ (2) Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller ~~immediately~~ without undue delay after the identification ~~establishment~~ of a significant and material personal data breach. (3) The notification referred to in paragraph 1 must, where available, at least: (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; ~~(c) recommend measures to mitigate the possible adverse effects of the~~

data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach.	~~personal data breach;~~ (d) describe, if possible, the consequences of the personal data breach; (e) describe, if possible, the measures proposed or taken by the controller to address the personal data breach and/or mitigate its adverse effects.

Justification:

Notifying data breaches is already an obligation imposed by the ePrivacy Directive. Therefore, we welcome the extension of the data breach notification obligation to all data controllers, which will ensure both a level playing field between providers and a consistent protection framework for European data subjects. However, the requirements imposed by both the ePrivacy Directive and the draft Regulation should be aligned to avoid a dual notification obligation for e-communications providers and a different level of protection for data subjects.

Telefónica would suggest some modifications in the current wording in order for these provisions to be not only feasible, but effective.

The current definition of "personal data breach" requires further clarification, especially regarding the source of the "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data…", currently defined in Art. 4.9.

We understand that the responsibilities placed on the controller in relation to a personal data breach should apply only in situations in which there is a breach of security in the controller's systems or networks, or due to some action, decision, technical or security error, or other cause associated with the systems and/or activities of the controller.

It should not apply in cases such as phishing, when a data subject voluntarily grants access to their personal information to a third party based on deceptive activity by that third party.

A "24 hours requirement" to notify to the Supervisory Authority is arbitrary and unjustified. Notification is only useful after a first technical verification of the cause. This is often not possible in 24 hours and it is distracting from the real and critical objective of fixing the data breach as soon as possible.

Moreover, the DPAs will not have the resources to deal with it and the general public will get "notification fatigue" undermining the core policy objective of notifications. This very significant burden introduced on EU businesses would then simply result in the paralysis of the competent authorities. A more pragmatic approach is that a company must log all data breaches and that this log can be inspected by the DPA at any time, but that only more serious breaches have to be actively reported within a reasonable time frame.

To sum up, given the limited time frame for notifications and the potential

Proposed Amendment 19

Article 33 **Data Protection Impact Assessment**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(1) Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (2) The following processing operations in particular present specific risks referred to in paragraph 1: (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; […] (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale; (4) The controller shall seek the views of data subjects or their representatives on the intended	(1) Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller ~~or the processor acting on the controller's behalf~~ shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (2) The following processing operations in particular present specific risks referred to in paragraph 1: ~~(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;~~ […] (c) monitoring publicly accessible areas~~, especially when~~ using optic-electronic devices (video surveillance) on a large scale; ~~(4) The controller shall seek the views of data subjects or their~~

processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	~~representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.~~

Justification:

Data controllers should have flexibility in determining risks under the principle of accountability. Data controllers know the particularities of their products, services or sectors and can better adapt DPIAs to their needs.

A PIA is naturally a duty of the controllers, therefore, imposing this obligation also on processors should be questioned as it could be even more counterproductive, diluting the liabilities between the data controller and the data processor. This poses a particular problem in the area of cloud, where more than ever the responsabilities and roles of the data controller and the data processor shall be clearly differentiated.

We call for the removal of the obligation to conduct a PIA of a processing based on profiling, as we do not agree with the fact that profiling per se presents “specific risks”.

Article 33 (4) obliges data controllers to seek the views of data subjects or their representatives (e.g., consumer organisations) on the intended processing of their personal data. This obligation is disproportionate and would create commercial concern for companies developing new products and services in highly competitive markets. Therefore, we suggest its deletion.

Proposed Amendment 20

Article 43 **Transfers by way of binding corporate rules**	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they: (a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees; (b) expressly confer enforceable rights on data subjects; (c) fulfil the requirements laid down in paragraph 2.	1. (New)One supervisory authority shall in accordance with the consistency mechanism set out in Article 58 and through a single act of approval authorize binding corporate rules for a group of undertakings. 2. (New)Those rules will allow multiple intercompany international transfers in and out of Europe, provided that they: (a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees; (b) expressly confer enforceable rights on data subjects; (c) fulfil the requirements laid down in paragraph 2.

Justification:

Telefónica welcomes the recognition of the concept of "group of undertakings" as well as the Binding Corporate Rules (BCRs) for data transfer within a Group of undertakings.

BCRs already exist under the current regulatory framework; however they do not work in practice. They have proven to be too onerous and inflexible to be a workable solution, because companies were requested to receive the green light from all national DPAs of those Member States where they were active. That implied an extraordinary administrative burden for companies.

The BCRs under the new Regulation must be designed to become the useful solution the Commission intends it to be. Therefore, to be a workable solution, Telefónica ask for a streamline approval process of the BCR's through which they allow one data protection Agency approval which in turn allow multiple intercompany international transfers in and out of Europe. In other words, just only one company of the Group of Companies is requested to receive green light from one DPA of one of the Member States.

Proposed Amendment 21

Article 44 Derogations	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
1 (h) the transfer is necessary for the purposes of the legitimate interests of the controller or processor, which cannot be qualified as frequent or massive, and where the .....”	1 (h) the transfer is necessary for the purposes of the legitimate interests of the controller or processor, ~~which cannot be qualified as frequent or massive, and where the .....”~~

Proposed Amendment 22

Article 51 Competence	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
2. Where the processing of personal data takes place in the context of the activities of an establishment [...], the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.	2. Where the processing of personal data takes place in the context of the activities of an establishment [...], the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor respectively in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

Justification:

According to our understanding the one-stop shop criteria depend on where the company providing the service is established.

There is, however, one situation that is not quite clear under the proposed Art. 51. The specific example Telefónica is thinking about is the following:

- Telefónica's cloud services are provided by its UK based subsidiary Telefónica Digital, so the ICO is the relevant authority;
- However, this service is marketed by Telefónica's Operating Businesses across the EU. Telefónica Digital acts as a processor.
- In this case, the supervisory authority would also be the ICO for all matters related to the obligations of the processor and not the supervisory authority of the main establishment of the data controller.

Telefónica therefore would like to suggest an amendment to Art 51 by adding the word "respectively" with the aim of making clear that in these cases the supervisory authority for the processing activities of the processor should be the authority where the main establishment of the processor is located.

Proposed Amendment 23

Article 77 **Right to compensation and liability**	
Commission Proposal	Proposal (proposed new text in blue)
1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered. 2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage, to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24. 3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.	1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller ~~or the processor~~ for the damage suffered. 2. Where more than one controller ~~or processor~~ is involved in the processing, each controller ~~or processor~~ shall be jointly and severally liable for the entire amount of the damage, to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24. 3. The controller ~~or the processor~~ may be exempted from this liability, in whole or in part, if the controller ~~or the processor~~ proves that ~~they are~~ it is not responsible for the event giving rise to the damage.

Justification:

Liability should be maintained on the data controller as it is currently the case further to the Directive 1995/46/EC. The controller is the one who has the direct link with the data subject and is the one responsible vis-à-vis the data subject. If the controller considers any eventual damage was due to the processor's incorrect processing, the data controller will ask compensation from the processor. Furthermore, the controller and the processor normally establish the liability relationship in the contractrual arrangements, for cases where the processor does not act as requested by the data controller.

This article instead of helping data subjects creates confusion for controllers, processors and even more importantly for data subjects.

Proposed Amendment 22

Article 79 Sanctions	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(3) In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where: (a) a natural person is processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.	(3) In case of a 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: (a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).	(4) The supervisory authority ~~shall~~ may impose a fine up to 250.000 EUR~~, or in case of an enterprise up to 0,5 % of its annual worldwide turnover,~~ to anyone who, intentionally or negligently: (a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).
(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	(5) The supervisory authority ~~shall~~ may impose a fine up to 500.000 EUR~~, or in case of an enterprise up to 1 % of its annual worldwide turnover,~~ to anyone who, intentionally or

negligently: […] (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); (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: […] (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;	negligently: […] ~~(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);~~ (6) The supervisory authority ~~shall~~ may impose a fine up to 1.000.000 EUR or~~, in case of an enterprise up to 2 % of its annual worldwide turnover,~~ to anyone who, intentionally or negligently: […] ~~(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;~~

Justification:

Sanctions should not be automatically imposed. A margin of evaluation and assessment should be left for national DPAs to take into account the specific situations and the circumstances of a given infringement (eg. willingness to cooperate to solve the data breach, adoption of voluntary remedies, quality of the dialogue between the company and the DPA).

The word “shall” should be replaced by “may” in Articles 79.4, 79.5 and 79.6.

Sanctions must be proportionate to the risks and any privacy harms associated with the specific context of processing and only after consideration of all facts. This requires the development of objective criteria to guide DPAs. It also requires reconsideration of fines related to a company’s worldwide annual turnover, which is not directly related to the severity of the infringement and is therefore disproportionate.

Any reference to a percentage of “annual worldwide turnover” should be deleted. Such a criteria is unpredictable and would lead to uncertainty for companies. To ensure legal certainty, a maximum amount of fine should be established.

In terms of proportionality and considering the very high sanctions foreseen, some of the sanctions foreseen are seemingly not related to the severity of the infringement, therefore are not proportionate.

The Regulation should address non compliance that has harmful consequences for individuals. Sanctions should envisage enhancing the protection of privacy, rather than punishing failure of administrative requirements without impact for data subjects. The individual should be the protected interest, not the data itself.

Concrete examples of this lack of proportionality are Art. 79.5.f, Art. 79.6.h.