GENERAL DATA PROTECTION REGULATION SUGGESTIONS FOR AMENDMENTS

INDEX

DEFINITION OF PERSONAL DATA

(ARTICLE 4 (1))

BACKGROUND

While the current Directive 95/46/EC is centered around a definition of 'personal data', the proposed Regulation instead defines who is a 'data subject'. The change of approach is determined by the Commission's willingness to make the consumer the focal point of the reform. To ensure maximum protection of personal data, the Regulation lowered the threshold for identifying personal data stating that data are personal if "identifiable" by any "third party" ("by any other natural or legal person") with the consequence of virtually making any information to qualify as personal.

PROBLEM(S) IDENTIFIED

The personal data definition proposed by the Commission has been considerably broadened to cover an unlimited amount of information, irrespective of their nature or the context in which they are processed or whether they are anonymised/pseudonymised or not, or whether the controller had any intention to identify a user.

This is due to the fact that the relevant angle to determine 'identifiability' of a person is not limited, as has previously been the case, to the perspective of the controller, but has been extended to the perspective of 'any other natural or legal person', irrespective of the relationship with the controller. For instance, an IP address can arguably not be personal data to a website operator while it is for the access provider that assigned it. According to the current text proposal, the simple fact that a third party (in the example the access provider) is able to identify the individual on the basis of information available to him renders such information as personal *per se* also for the website provider.

This circumstance removes incentive for companies to invest in privacy enhancing measures as there will be no secure way to anonymise or pseudonymous information any longer. Coupled with the new "explicit consent" requirement, this broad definition of personal data is particularly problematic, as virtually any information will require the users' explicit consent. Rules applying to such a broad definition risk to be unworkable in practice and to generate legal uncertainty.

Finally, by mentioning ‘online identifiers’ ‘location data’, the definition of data subject is not technologically neutral.

PROPOSED SOLUTION(S)

In order to make the definition of personal data workable in practice, a “context based approach” should be introduced in the definition. This means that the personal character of the data should depend on who is processing it, how, and for what purpose:

- Data should only be considered as personal where it is reasonably likely that, based on the context, the data controller or processor has the intention to use data in a way that requires personal identification of the data subject or where there is a realistic risk of such identification.
- The reference to “online identifier” and “location data” is not technology neutral and should be deleted. Additionally, as to online identifiers, if we consider tehm to be IP-addresses, they are already included in the broader definition of “identification number”.
- A clear definition of pseudonymous data should be introduced. Also, in cases where data is used to distinguish between users, rather than identifying them, the data should not be considered as personal.
- Anonymised data should be defined in the text as not being personal data.
- The lawful grounds for processing (article 6) should also be modified to reflect the specificities of pseudonymous and anonymous data.
- Finally, the reference to delegated acts should be deleted.

General Data Protection Regulation ***Article 2***	**Amendments** ***Article 4***
Definitions	***Definitions***
For the purposes of this Regulation:	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;	(1) 'data subject' means an identified natural person or a natural person who can**, based on the context of the specific processing**, be identified, directly or indirectly, by means reasonably likely to be used by the controller **or the processor** ~~or by any other natural or legal person~~, **including** ~~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; **these means** ~~factors~~ **as such need not necessarily be considered as personal data in all circumstances;**
(2) 'personal data' means any information **relating to** a data subject;	(2) 'personal data' means any information **used to directly or indirectly identify** ~~relating to~~ a data subject; **NEW (3) Pseudonymous data means any personal data that has been collected, altered or otherwise processed in such a way that any personal characteristics, such as the name or other personal identifiers, are replaced with a code so that the data**

	subject can no longer be identified or that identifiability would require a disproportionate amount of time, cost and effort.
	NEW (4) "Anonymous data" means any information that has been collected, altered or otherwise processed in such a way that it cannot be attributed to a data subject.
	RECITALS
	NEW
	Pseudonymisation is the process of disguising identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity (i.e. research and statistics). Pseudonymisation can be done in a retraceable way by using correspondence lists for identities and their pseudonyms or by using two-way cryptography algorithms for pseudonymisation. Key-coded data are a classical example of pseudonymisation. Information relates to individuals that are earmarked by a code, while the key making the correspondence between the code and the common identifiers of the individuals (like name, date of birth, address) is kept separately.
(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used **either** by the controller **or by any other person** to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.	(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means **that are technically feasible, do not involve a disproportionate effort, and are** likely reasonably to be used ~~either~~ by the controller or **the processor** ~~by any other person~~ to identify the individual**, based on the context of the specific processing. In cases where data is used to distinguish between data subjects, rather than identifying them, these data shall be considered as pseudonymous personal data.** The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable**, taking into account the technological "state of the art".**
Article 2	**Article 2**
Material Scope	**Material Scope**
(…)	(…)

2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; (b) by the Union institutions, bodies, offices and agencies; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; (b) by the Union institutions, bodies, offices and agencies; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; **(f) that has been rendered anonymous**
Article 6	**Article 6**
Lawfulness of processing	***Lawfulness of processing***
1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks;	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks; **NEW (g) processing is necessary for the implementation of technical security**

measures or mechanisms to ensure the protection of personal data or for the prevention of fraud;

NEW (h) processing of pseudonymous data is lawful, provided that the data subject does not object;

NEW (i) processing of anonymised data is lawful at all times.

(…)

(…)

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.~~

MAIN ESTABLISHMENT

(ARTICLES 3 AND 4 (13))

BACKGROUND

With the proposed Regulation, the Commission intends to truly harmonise the rules governing the processing of personal data in the European Union and clarify the rules on applicable law. It is proposed to put in place one single set of data protection rules (i.e. the Regulation) applicable throughout the EU coupled with a so called “one stop shop” enforcement system, establishing the competence of one single national data protection authority (DPA), in particular where companies operate and process personal data in more than one Member State. Purpose of the creation of the one-stop-shop is to achieve consistent application of the Regulation throughout all Member States, provide legal certainty and reduce administrative burdens for data controllers and processors. The one stop shop is determined on the basis either of the “main establishment” of a company within the EU or, where a company’s main establishment is outside the EU, the “place of residence of the consumer” who is being offered products or services or whose behavior is being monitored. As concerns the second circumstance, the idea is to extend the extra territorial application of the Regulation to any processing of personal data even if carried in a third country.

PROBLEM(S) IDENTIFIED

- Article 4 (13) defines the “main establishment” differently for data controllers vis-à-vis to data processors. **As regards the controller,** main establishment means 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 such decisions 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. The reasoning behind this different regime for controllers and processors is, however, unclear.

- Article 51(2) of the Regulation foresees that the competent authority, providing the one-stop shop, is the supervisory authority of the Member State in which the controller or processor has its main establishment. Consumers, however, will be able to issue a complaint in their own country even if the controller or processor is established elsewhere (Article 73). However, the Regulation is silent on the question of how supervisory authorities should act when receiving a complaint concerning a controller whose main establishment is in a different country. Furthermore, it is unclear how cooperation between the different data protection authorities would work in practice, so putting at risk the creation of a level playing field in the EU.

- The fact that the Regulation applies to any processing of personal data in the context of activities of an establishment in the Union, even if this processing takes place outside of the EU, means that EU rules apply whenever actors operating in third countries target EU users (Article 3). It could be particularly complex for international companies operating from different geographical regions of the world if they have to implement potentially conflicting legislation, i.e. their own national law and within the EU.

- Applicable law criteria in those cases where national law builds on or exempts from the Regulation should be clearly laid out.

PROPOSED SOLUTION(S)

- A uniform definition of main establishment for both data controller and processor should be considered

- The term 'main establishment' requires further clarification. It could be understood as the company's central administration. Objective criteria need to be elaborated to define it and a clear reference to the role of the "representative" for those companies established outside the EU should be foreseen.

- For groups of undertakings, the designation of the 'main establishment' should apply to all entities part of the group established in the Union. The lead DPA for the company's main establishment should be competent to supervise all processing carried out by all entities of the group as far as they are subject to the Regulation

- The cooperation and consistency mechanism between DPAs needs to be strengthened further to allow for a true one stop shop. DPAs who receive a complaint or have others reasons to investigate with respect to a controller whose main establishment is located in a Member State different from the consumer's place of residence should be required to refer the matter to the lead DPA. The latter should be leading for all privacy matters concerning companies with a main establishment in its jurisdiction

- The extra territorial application of the Regulation vis-à-vis controllers established in third countries processing personal data of EU citizens should be clarified to only cover situations where goods and services are specifically targeted at EU citizens. In particular[1], due account must be taken of the jurisprudence of the European Court of Justice.

General Data Protection Regulation ***Article 4*** ***Definitions***	**Amendments** ***Article 4*** ***Definitions***
(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 **and the processor**, the place of **their** ~~its establishment~~ **central administration** in the Union**, or in the absence of such administration, the place** where the main decisions as to ~~the purposes, conditions and means of~~ the processing of personal data are taken, **in accordance with their respective competences**; 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 **controller or processor has its representative** ~~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;~~

1 In the Hotel Alpenhof GesmbH v Oliver Heller case (C-144/09), the ECJ elaborated objective criteria that can be used to assess the intention of an operator to expressly target EU citizens such as the use of a language or a currency other than the language or currency generally used in the country in which the operator is established, the possibility of making and confirming the reservation in that other language, the use of a top-level domain name with the .eu suffix or other than that of the country in which the merchant is established.

	NEW 13 (a) The designation of the 'main establishment' should apply to all entities part of a group of undertakings established in the Union
	NEW 13 (b) The controller and processor shall communicate their main establishment to the competent supervisory authority.
Article 51	***Article 51***
Competence	***Competence***
(…)	(…)
2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.	2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States **and, in the case of a group of undertakings, of any member of the group,** without prejudice to the provisions of Chapter VII of this Regulation.
	NEW 3. **Where the controller or processor has designated a representative in the Union pursuant to Article 25, the supervisory authority of the establishment of the representative in accordance with Article 25.4 shall be competent for the supervision, in all Member States, of all processing activities of that controller or processor.**
(…)	(…)
Article 3	***Article 3***
Territorial scope	***Territorial scope***
(…)	(…)
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: **(a)** the **offering** of goods or services to such data subjects in the Union; **or** **(b) the monitoring of their behaviour.**	2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities**, including the monitoring of behaviour,** are related to ~~(a)~~ the **targeted** offering of goods or services to such data subjects in the Union; ~~or~~ ~~(b) the monitoring of their behaviour.~~

(…)

RECITAL

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, **or to the monitoring of the behaviour of such data subjects**.

(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. **The main establishment of the processor should be the place of its central administration in the Union.**

(…)

RECITAL

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities**, including the monitoring of the behaviour of such data subjects,** are related to the **targeted** offering of goods or services to such data subjects,~~, or to the monitoring of the behaviour of such data subjects~~ **in accordance with the jurisprudence of the European Court of Justice and based on objective criteria that can be used to assess the intention of an operator to target EU citizens such as the use of a language or a currency other than the language or currency generally used in the country in which the operator is established, the possibility of making and confirming the transaction in that other language, the use of a top-level domain name with the .eu suffix or other than that of the country in which the operator is established.**

(27) The main establishment of a controller **or a processor** ~~in the Union~~ **should be the place of their central administration which** should be determined according to **the following** objective criteria**: the location of the group's European headquarter or the location of the company within the group with delegated data protection responsibilities. In the absence of a central administration, the main establishment is the place where the main decisions as to the** ~~purposes, conditions and means of~~ **processing are taken.** ~~and,~~ **As regards the controller, the main establishment** should imply the effective and real exercise of management activities determining the main decisions as to the ~~purposes, conditions and means of~~ processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or

processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. ~~The main establishment of the processor should be the place of its central administration in the Union.~~

CONSENT

(ARTICLE 4 (8))

BACKGROUND

The Regulation sets stricter thresholds as compared to the current Directive 95/46 by defining consent as "freely given specific, informed and explicit indication" of an individual's wishes. The requirement for consent to always be “explicit”, irrespective of the context for which consent is being obtained or the risks involved in the processing operation for the individual, could be construed as always requiring a "yes" response to having one's personal data processed. According to Recital 25 of the Regulation, explicit consent can be provided “either by a statement or by a clear affirmative action”, but would not encompass consent implied from individuals' actions or behaviour.

PROBLEM(S) IDENTIFIED

The proposed approach is too formalistic and rigid, creates uncertainty and practical problems, without adding anything to individuals’ data protection. In fact the current and future technology environment allows for consent to be inferred or implied from users’ actions. However, this would not meet the threshold set in Article 4 (8) for explicit consent. This is even more restrictive for Internet operators if one considers that - in conjunction with Article 7 (Conditions for consent) - an increased reliance is introduced on (explicit) consent as the preferred legal basis for data processing over other possible grounds as foreseen in Article 6 (Lawfulness of processing), i.e. processing for the performance of a contract; for compliance with legal obligation; for the purposes of a legitimate interest pursued by a controller.

Finally, article 7 (4) states that consent cannot be used in case of ‘significant imbalance’ between the position of the data subject and the controller. This provision is confusing and might risk creating a situation where companies with bargaining power will never be able to rely on consent.

PROPOSED SOLUTION(S)

A context based approach should be introduced allowing the controller to select the most appropriate way/mechanism of providing information, obtaining meaningful consent and offering control to data subjects, depending on the context of the specific data use and the risks involved for data subjects. The “explicit” requirement should be replaced by a more flexible criterion that, while guaranteeing a higher level of protection of data subjects, would make the Regulation more technology neutral and, particularly, not chill technology innovation.

General Data Protection Regulation	**Amendments**
Article 4	*Article 4*
Definitions	***Definitions***
For the purposes of this Regulation:	For the purposes of this Regulation:
(8) 'the data subject's consent' means any freely given specific, informed and **explicit** indication of his or her wishes by which the	(8) 'the data subject's consent' means any freely given specific, informed and **verifiable** ~~explicit~~ indication of his or her wishes by which the data subject, either by a statement or **through his behavior** ~~by a clear affirmative~~

data subject, either by a statement or **by a clear affirmative action**, signifies agreement to personal data relating to them being processed;	~~action~~, signifies agreement to personal data relating to them being processed;
Article 7 ***Conditions for consent*** 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.	*Article 7* ***Conditions for consent*** 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. **If the data processed by the controller do not permit the controller to identify the data subject, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of proving his consent.**
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.	2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
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 **in accordance with EU and Member States' law**.
RECITAL	*RECITAL*
(25) Consent should be given **explicitly** by any appropriate method enabling a freely given specific **and** informed indication of the data subject's wishes, either by a statement or **by a clear affirmative action by the data subject**, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or **conduct** which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent	*(25) Consent should be given ~~explicitly~~ by any appropriate method enabling a freely given specific, ~~and~~ informed **and verifiable** indication of the data subject's wishes. **This indication can be given** either by a statement **(including a clear affirmative action)** or **through the behavior of the data subject,** ~~by a clear affirmative action by the data subject,~~ ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or **behavior** ~~conduct~~ which clearly indicates in this context*

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.

the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.

(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. ***If the data processed by the controller, however, do not permit the controller to identify the data subject, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of proving his consent****. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.*

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent ***without detriment****.*

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent ~~without detriment~~.

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

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

DATA PROTECTION AND INTERMEDIARY LIABILITY

(ARTICLE 2(3))

BACKGROUND

Both the EU data protection rules and the intermediary liability regime of the E-Commerce Directive are of major importance to online intermediaries. However, the interpretation of, and interplay between, these two legal instruments is unclear, leading to a number of legal challenges for Internet operators. Indeed, Article 1 (5) (b) of the E-commerce Directive states that the Directive does not apply to "questions relating to information society services covered by Directive 95/45/EC (…) [Data Protection Directive]". There is a risk that authorities could make online intermediaries fully liable for data protection violations by third parties, even in the case where the intermediary “expeditiously" takes down illegal content upon being made aware of the breach of data protection rules, in the meaning of Article 14 of the E-Commerce Directive.

PROBLEMS IDENTIFIED

As it currently stands, it is not clear whether the protection granted by the E-Commerce Directive does apply to circumstances where an intermediary is dealing with personal data. The lack of confirmation deprives the intermediary of a needed legal protection. In order to address this shortcoming, the Commission introduced an explicit reference in the scope of the Regulation referring to the E-Commerce Directive (Article 2, 3). This allows an intermediary to be subject to data protection obligations only if it is acting as a controller because only a controller is in the position to take decisions related to the processing of personal data. Accordingly, while service providers should be held liable for their own collection and use of personal data of individuals (i.e., when they act as controllers), this same liability needs to be limited where it concerns data protection issues related to third party use of online services.

PROPOSED SOLUTION(S)

In order to address the legitimate concerns of the intermediaries, a clarification of the scope of the Regulation to the E-Commerce Directive regime should be introduced in the text.

Directive 95/46/EC	**General Data Protection Regulation** RECITAL ***NEW*** **The liability limitations of the Directive on Electronic Commerce 2000/31/EC are horizontal in nature and therefore apply to relevant activities of all information society service providers. This Regulation establishes the rules for the processing of personal data, determines what constitutes a privacy and data**

protection infringement, while the Directive on Electronic Commerce sets out the conditions by which an information service provider is liable for third party infringements of the law. In the interest of legal certainty for European citizens and businesses, the clear and distinct roles of the two instruments need to be respected.

This consistency can be ensured by holding service providers, other than controllers, acting only as conduits or merely providing automatic, intermediate and temporary storage or storage of information provided by a recipient of the service or allowing or facilitating the search of or access to personal data, shall not be responsible for personal data transmitted or otherwise processed or made available by or through them.

RIGHT TO BE FORGOTTEN

(ARTICLE 17)

BACKGROUND

One of the main goals of the Regulation is to put data subjects in control of their personal data. In addition to the existing general right to erasure under the current Directive 95/46/EC (where article 12 requires controllers to erase personal data at the request of the data subject where the data can no longer be processed in accordance with the law), the Regulation tries to reinforce this right for the online environment. Indeed it requires controllers that have made information available about an individual public (whether this happened upon request of the individual or not) to inform "third parties" that are processing the data of the request of the data subject to erase any links to, or copy, or replications of the data (so called Right to be Forgotten).

PROBLEM(S) IDENTIFIED

The obligation for data controllers to inform third parties that are processing the data of the request of the data subject is vague as to the procedure to be used and risks to be extremely difficult to implement in practice. For an Internet provider it is not always possible to identify who has accessed the data and might be processing it. Furthermore, the fact that the obligation also concerns data that were consciously made public by the user makes it even more unreasonable to require the Internet provider to inform every potential "third party" (concept not defined by the Regulation) of the wishes of the data subject to have the data deleted. In that case, the obligation to inform third parties should lie with the data subject instead of the controller. Finally, the Regulation states that where erasure is carried out, data cannot be processed further. The complete removal of all data, however, could negatively affect the capability of the controller to verify or prove compliance with the requests of the data subject.

PROPOSED SOLUTION(S)

The proposed rules regarding the right to be forgotten and corresponding obligations for controllers should be clarified. The interest of the user to be forgotten and the legitimate interests pursued by the controller for processing need to be balanced.
The obligation for controllers should only apply vis-à-vis recipients of data to whom the controller has transferred the data (i.e. when a contractual relation exists). This situation, however, is already covered by article 13, which foresees that "the controller shall communicate any rectification or erasure to each recipient to whom the data have been disclosed unless this proves impossible or involves a disproportionate effort". Therefore article 17 (2) does not add anything to what already exists in the proposed Regulation and should be deleted.
Additionally, article 17 (8) (saying that where erasure is carried out, the data cannot otherwise be processed) should be modified in a way to allow the controller to verify or prove compliance with the requests of the data subject, or to allow processing for billing purposes.

General Data Protection Regulation	**Amendments**
Article 17	
Right **to be forgotten and** to erasure	*Article 17* *Right ~~to be forgotten and~~ to erasure*

(…)	(…)
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. 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.~~
(…)	*(…)*
8. Where the erasure is carried out, the controller shall not otherwise process such personal data**.**	8. Where the erasure is carried out, the controller shall not otherwise process such personal data**, unless to prove compliance with the data subject's request or to allow processing for billing purposes.**
RECITAL (53) Any person should have the right to have personal data concerning them rectified **and a 'right to be forgotten'** where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.	RECITAL (53) Any person should have the right to have personal data concerning them rectified ~~and a 'right to be forgotten'~~ where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law**, to prove compliance with the data subject's request, to allow processing for billing purposes** or where there is a reason to restrict the processing of the data instead of

erasing them.

(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

~~(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.~~

PRIVACY BY DEFAULT / PRIVACY BY DESIGN

(ARTICLE 23)

BACKGROUND

The principles of data protection by design and data protection by default have been included explicitly in the proposed Regulation. Article 23 obliges the controller to implement processes allowing for data protection aspects to be carefully considered both at design and implementation stage of products and services. The new provision (article 23 (1)) frames the obligation of the controller to implement these principles both at the time of the determination of the means for processing and at the time of the processing itself, and to do so in the context of "the state of the art and the cost of implementation" while ensuring that "appropriate technical and organisational measures and procedures" are in place.

PROBLEM(S) IDENTIFIED

Article 23 (2) which deals with privacy by default, is redundant as it is limited to repeating the principle of "data minimisation" already contained in Article 5 of the Regulation (i.e. data retention/collection should be limited to those data which are strictly necessary for the processing). Additionally, the article mandates that the collection of data by default be justified according to "each specific purpose of the processing", ignoring the fact that some perfectly legitimate and socially desirable uses data may be unknown at the time of collection. Finally, the new provision empowers the Commission to "lay down technical standards". The imposition of such standards would create legal, investment and development uncertainty and hinder, rather than promote, user privacy.

PROPOSED SOLUTION(S)

- Privacy by design should be implemented by industry according to the means it has at its disposal, based on the most appropriate mechanisms for the specific business model and on the accountability principle. Therefore, the reference to delegated acts should be deleted.

- Any reference to privacy by default should be deleted as Article 5 of the Regulation already set obligations on data minimisation.

General Data Protection Regulation ***Article 23***	**Amendments** ***Article 23***
Data protection by design and by default	***Data protection by design and by default***
(…)	(…)
2. The controller shall implement mechanisms for ensuring that, **by default**, personal data shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data **only those personal data are processed which are necessary for each**	2. The controller shall implement mechanisms for ensuring that, ~~by default,~~ personal data shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data ~~only those personal data are processed which are necessary for each specific purpose of the~~

specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

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

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

(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by **design and data protection by default**.

~~processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.~~

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

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

(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design ~~and data protection by default.~~

SANCTIONS

(ARTICLE 79)

BACKGROUND

The Commission wishes to strengthen the role of national Data Protection Authorities (DPAs) by enabling them to issue fines that are sufficiently dissuasive. While Directive 95/46EC left it to the Member States to lay down in national law the sanctions to be imposed in case of infringement (Article 24), the proposed Regulation foresees specific sanctions to be issued by national DPAs.

PROBLEM(S) IDENTIFIED

Article 79 of the proposed Regulation foresees that, depending on the violation, companies can be sanctioned with a fine ranging from 0,5% to up to 2% of their annual worldwide turnover. This approach would be burdensome for SMEs but also create an uneven playing field between multinational companies and companies without global outreach.

PROPOSED SOLUTION(S)

The reference to companies' global turnover should be deleted and the turnover should be capped at the maximum amount that can be imposed.
The word 'shall' in article 79 (4 – 6) should be replaced by 'may' in order to provide DPAs with flexibility in deciding whether or not it is necessary to impose a fine at all.
The proportionality of breaches allocated to the highest category of sanction should be re-considered (i.e. breaching the provision requiring maintenance of documentation triggers a fine of 0.5% of global annual turnover, which is disproportionate considering that this is a simple administrative fault without substantial damage to individuals. In general fines should be reserved to most substantial and severe breaches).
As regards the calculation of the amount of the sanction, the following circumstances should be considered:

- the actual damage suffered by the data subject or the actual risk of suffering a damage;
- the presence of aggravating circumstance such as repeated violations, refusal to cooperate or deliberate violations causing substantial damage;
- the presence of mitigating circumstances such as measures taken by the controller or processor to ensure compliance with the Regulation, immediate termination of the violation upon knowledge or cooperation with enforcement processes.

Finally, the consistency mechanism should be used to cover divergences in the application of the administrative sanctions.

General Data Protection Regulation Article 79	**Amendments** Article 79
Administrative sanctions	**Administrative sanctions**
(…)	(…)
2. The administrative sanction shall be in each individual case effective, proportionate and	2. The administrative sanction shall be in each individual case effective, proportionate and

dissuasive. **T**he amount of the administrative fine shall be **fixed** with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.	dissuasive. **The decision to impose an administrative fine or t**~~T~~he amount of the administrative fine shall be ~~fixed~~ **determined** with due regard to the nature, gravity and duration of the breach, **the actual damage or risk of suffering a damage caused to the data subject,** the intentional or negligent character of the infringement, **the immediate termination upon knowledge of the infringement,** the degree of responsibility of the natural or legal person and of previous breaches by this person, **the repeated violation of the same provision, the refusal to cooperate,** the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.
(…)	(…)
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 ~~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);	(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).	(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4)**;**
	NEW (c) provides not transparent information and communication relating to the processing of personal data to the data subject in violation of Article 11.
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 ~~shall~~ **may** impose a fine up to 500 000 EUR, to anyone who~~, intentionally or negligently~~:
(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to **Article 11**, Article 12(3) and Article 14;	(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to ~~Article 11~~, Article 12(3) and Article 14;

(…)	(…)
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 ~~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~~:
(…)	(…)
(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;	(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, **except from §2**, 23 and 30;
(…)	(…)
RECITAL	RECITAL
(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation **should** indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity **and** duration of the breach. The consistency mechanism **may also** be used to cover divergences in the application of administrative sanctions.	(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation ~~should~~ indicate**s** these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity~~, and~~ duration of the breach**, the actual damage or risk of suffering a damage caused to the data subject, the intentional or negligent character of the infringement, the immediate termination upon knowledge of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the repeated violation of the same provision, the refusal to cooperate, the technical and organizational measures and procedures implemented pursuant to Article.** The consistency mechanism ~~may~~ **should** ~~also~~ be used to cover divergences in the application of administrative sanctions.