Amendements proposed by

La Quadrature du Net

on the ePrivacy Regulation

16th June 2017

Recital 2

The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc.	~~The content of e~~Electronic communications data may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. ~~Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata~~ These data includes~~s~~ **text, voice, videos, images, sounds, the IP and MAC addresses of end-users,** the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call, etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc.

Justification:

In principle, content and metadata should benefit from the same level of protection. It has been shown many times that metadata give as much relevant information as content linked to end-users private life (see: https://techcrunch.com/2016/05/17/stanford-quantifies-the-privacy-stripping-power-of-metadata/ or https://www.privacyinternational.org/node/53). There is no justification anymore to make a difference on the level of pretection for metadata and content.

Recital 4

Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data may include personal data as defined in Regulation (EU) 2016/679.	Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data may include **and, as regards natural persons, are always** personal data as defined in Regulation (EU) 2016/679.

Justification:

Clarifies which electronic communications data are personal data.

Recital 5

The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore does not lower	The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore does not lower

the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation.	the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation. **Where both this Regulation and the Regulation (EU) 2016/679 may apply to the same processing, this Regulation only shall apply.**

Justification:

Clarifies how the two Regulations will apply together.

Recital 7

The Member States should be allowed, within the limits of this Regulation, to maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. Therefore, the margin of discretion, which Member States have in this regard, should maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.	~~The~~ Member States should be allowed, within the limits of this Regulation, to maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. Therefore, ~~the margin of discretion, which Member States have in this regard, should maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.~~ **Member States may only introduce provisions increasing end-users' privacy.**

Recital 8

This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to software providers permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing commercial communications or collect information related to or stored in end-users' terminal equipment.	This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to software providers permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing commercial communications or collect information related to or stored in end-users' terminal equipment **or use the processing capabilities of such terminal equipment**.

Justification:

Limiting how the processing capabitlities of the terminal equipment of end-users may be used should be clearly included in the broad scope of this Regulation. This recital is not clear on this point as it stands.

Article 2

1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.	1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information **and processing capabilities** related to the terminal equipment of end-users.
2. This Regulation does not apply to:	2. This Regulation does not apply to:
(a) activities which fall outside the scope of Union law;	(a) activities which fall outside the scope of Union law;
(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;	(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European

(c) electronic communications services which are not publicly available;	Union;
	~~(c) electronic communications services which are not publicly available;~~
(d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;	(d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

Justification:

Services not publicly available are excluded from the scope of telecommunications regulations for reasons specific to such regulations (for instance, it would be unjustified to impose access obligations on networks not publicly available). However, this distinction is irrelevent as regards the confidentiality of communications: all communications should be protected equally, irrespective of end-users' location. Therefore, electronic communications services which are not publicly available should remain within the scope of this regulation.

Otherwise, excluding them from this scope would allow companies to monitor how their employees are using their access to the network, which is unacceptable: companies only need to assess the work done by their employees, not to monitor each of their actions.

Article 3

1. This Regulation applies to:	1. This Regulation applies to:
a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;	a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;
b) the use of such services;	b) the use of such **electronic communications** services **by end-users located in the Union, irrespective of whether a payment of the end-user is required;**
c) the protection of information related to the terminal equipment of end-users located in the Union.	c) the protection of information **and processing capabilities** related to the terminal equipment of end-users located in the Union.

Justification:

The scope defined by the European Commission is ambigious: it is not perfectly clear whether services provided from outside the Union to end-users located in the Union fall within the scope of the Regulation. This precision is necessary in order for this Regulation to provide for the same territorial scope as the GDPR.

Article 4

2. For the purposes of point (b) of paragraph 1, the definition of ‘interpersonal communications service’ shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.	For the purposes of point (b) of paragraph 1**,:**
	(a) the definition of ‘electronic communications service’ shall include services providing access to the internet and which are not publicly available ;
	(b) the definition of ‘interpersonal communications service’ shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

Justification:

Services not publicly available are excluded from the scope of telecommunications regulations for reasons specific to such regulations (for instance, it would be unjustified to impose access obligations on networks not publicly available). However, this distinction is irrelevent as regards the confidentiality of communications: all communications

should be protected equally, irrespective of end-users' location. Therefore, electronic communications services which are not publicly available should remain within the scope of this regulation.

Otherwise, excluding them from this scope would allow companies to monitor how their employees are using their access to the network, which is unacceptable: companies only need to assess the work done by their employees, not to monitor each of their actions.

Recital 13

The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.	The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to ~~an undefined group of~~ end-users, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and ~~public~~ communications networks**, irrespective of whether these services and networks are publicly available or not**. ~~In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.~~

Justification:

Services not publicly available are excluded from the scope of telecommunications regulations for reasons specific to such regulations (for instance, it would be unjustified to impose access obligations on networks not publicly available). However, this distinction is irrelevant as regards the confidentiality of communications: all communications should be protected equally. irrespective of end-users' location. Therefore, electronic communications services which are not publicly available should remain within the scope of this regulation.

Otherwise, excluding them from this scope would allow companies to monitor how their employees are using their access to the network, which is unacceptable: companies only need to assess the work done by their employees, not to monitor each of their actions.

Article 4

3. In addition, for the purposes of this Regulation the following definitions shall apply:	3. In addition, for the purposes of this Regulation the following definitions shall apply:
a) ‘electronic communications data’ means electronic communications content and electronic communications metadata;	a) ‘electronic communications data’ means electronic communications content and electronic communications metadata;
b) ‘electronic communications content’ means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;	b) ‘electronic communications content’ means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;
c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device	(c) ‘electronic communications metadata’ means data processed**, generated or transmitted** ~~in an~~ **by an** electronic communications ~~network~~ **service** for the purposes of **sending,** transmitting**,** ~~distributing~~ or **receiving** ~~exchanging~~ electronic communications content; including data used to trace and identify the

generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;	source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;

Justification:

As its stands, the definition of metadata is limited to the data processed on the network by telecommunications operators (acting on layer 3, "transmission"- See the OSI model https://en.wikipedia.org/wiki/OSI_model). As such, it excludes from the scope of this Regulation the metadata generated and used by interpersonal communications services (Over The Top services – OTT) on higher level ("application" and "content").

Typically, the header of emails ("from:", "to:", "date:") are not processed "on the network" but only on the "application" layer by OTT and, as such, are not covered by the current definition.

Recital 14

Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.	Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata **from the perspective of Internet access providers** and therefore be subject to the provisions of this Regulation. **Data generated, processed or transmitted by interpersonal communications services for the purpose of sending, transmitting or receiving such communications should be considered as electronic communications metadata from the perspective of the providers of these services but should still be considered as electronic communications content from the perspective of Internet access providers.** Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.

Justification:

The definition of metadata depends on which layer of the network is considered. On layer 3 ("transmission" - See the OSI model https://en.wikipedia.org/wiki/OSI_model), the metadata and the content processed by OTT on higher level ("application" and "content") are all transmitted together in TCP/IP packets. Telecommunications operators make no distinction between the metadata and the content processed by OTT. From the perspective of operators, these data are the "content" transmitted on the network.

This recital should make this technical clarification.

Recital 15

Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.	Electronic communications data should be treated as confidential. This means that any interference with ~~the transmission of~~ electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. **Interferring means to process electronic communications data for any purpose not requested by all end-users concerned, whether such process is carried out before, during or after the transmission of communications.** ~~The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee.Interception of~~ **Interference with** electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. ~~Interception~~ **Interference** also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in ~~interception~~ **interference** have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of ~~interception~~ **interference** include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.

Justification:

As it stands, this recital may limit the scope of article 5 to interferences which only occurs durring the transmission of communications. This would prevent communications data from being protected before and after the transmission. Thus, this rectial needs clarification.

Article 6

1. Providers of electronic communications networks and services may process electronic communications data if:	1. Providers of electronic communications networks and services may process electronic communications data if:
(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or	(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or
(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.	(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.
	(c) if all end-users concerned have given their consent to the processing of their electronic communications data for one or more specified purposes, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the

	consultation of the supervisory authority.
2. Providers of electronic communications services may process electronic communications metadata if:	2. Providers of electronic communications services may process electronic communications metadata if:
(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 28 for the duration necessary for that purpose; or	(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 28 for the duration necessary for that purpose; or
(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or	(b) it is necessary for billing **or** calculating interconnection payments**; or**
	(c) it is necessary for detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services **and the recipient has given his or her consent to such processing**~~. ; or~~
(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.	~~(c)the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.~~
3. Providers of the electronic communications services may process electronic communications content only:	~~3. Providers of the electronic communications services may process electronic communications content only:~~
a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or	~~a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or~~
b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.	~~b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.~~

Justification:

Where based on consent, processing electronic communications data should only be authorised whith the consent of all end-users concerned by the communication, and no distinction should be made between processing content and metadata.

Furthermore, service providers detecting and stopping spams shall only be able to do so with the consent of end-users, who should be free to use anti-spam solutions provided by third-parties.

Recital 17

The processing of electronic communications data can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic	The processing of electronic communications **meta**data can be useful for businesses, consumers and society as a whole. ~~Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic~~

communications metadata, based on end-users consent. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to obtain end-users' consent to process electronic communications metadata, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.

~~communications metadata, based on end-users consent.~~ However, end-users attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to obtain all end-users' consent to process electronic communications ~~meta~~data, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. ~~Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure.~~ Where a type of processing of electronic communications ~~meta~~data, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.

Justification:

Location data are highly sensitive data especially as they enable one of the highest form of surveillance. They shall benefit from the higher level of protection.

Rectial 18

End-users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements. For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. Basic broadband internet access and voice communications services are to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice, or is

End-users may consent to the processing of their ~~meta~~data to receive specific services ~~such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements.~~ For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. ~~Basic broadband internet access and voice communications services are to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy.~~ Consent for processing data ~~from internet or voice communication usage~~ will not be valid if the data subject has no genuine and free choice, or is

unable to refuse or withdraw consent without detriment.	unable to refuse or withdraw consent without detriment. **As provided by article 7 of the Regulation (EU) 2016/679, consent is not freely given if it is required to access any service or obtained through insisting and repetitive requests. In order to prevent such abusive requests, end-ussers shall be able to order service providers to remember their choice not to consent.**

Justification:

Consent should be freely given for any kind of processing. The GDPR is not making any distinction between processing. This Regulation should not do this either.

Furthermore, end-users shall be protected from harassing requests leading to consent fatigue and to unfreely given consent.

Recital 19

The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.	~~The content of e~~**E**lectronic communications **data** pertain~~s~~ to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with ~~the content of~~ electronic communications **data** should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of ~~the content of~~ electronic communications **data**, this Regulation sets forth a presumption that the processing of such ~~content~~ data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. ~~The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service.~~ After electronic communications **data** ~~content~~ has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679. **Where communications data are stored by a third party, this third party shall encrypt from end to end any information which processing is not necessary to provide the service requested by the end-user.**

Justification:

Content and metadata should benefit from the same level of protection.

Providers shall encrypt from end to end communications where technically feasible.

Article 7

1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.	1. Without prejudice to point (b) of Article 6(1) ~~and points (a) and (b) of Article 6(3)~~, the provider of the electronic communications service shall erase electronic communications content ~~or make that data anonymous~~ after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.
2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.	2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata ~~or make that data anonymous~~ when it is no longer needed for the purpose of the transmission of a communication.

Justification:

Communication data are highly structured data that cannot be fully anonymised. Therefore, only the end-users should decide whether to be subject to such processing.

Furthermore, freedom of expression requieres that individuals should be free not to express their opinion and to choose how and where to express it. Using their communications for other purposes than the one they choose is against such freedom and should be strictly forbidden.

Article 8

Protection of information stored in and related to end-users' terminal equipment

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:	1.The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or	(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
(b) the end-user has given his or her consent; or	(b) the end-user has given his or her consent; or
(c) it is necessary for providing an information society service requested by the end-user; or	(c) it is necessary for providing an information society service requested by the end-user; or
(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.	(d)if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user **and rely only on information which cannot be associated with an identified or identifiable natural person**.
2.The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:	2.The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or	(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or
(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.	(b) ~~a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.~~ **the end-user has given his or her consent and no information emitted by his or her terminal equipment was used to request this consent;**
The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.
3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	~~3.The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.~~
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.	~~4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.~~

Justification

Being able to precisely locate individuals is one of the highest form of surveillance. It shall never occur without end-users' consent. Furthermore, service providers should not even be allowed to use information emitted by terminal equipments in order to directly send on their device the consent request, otherwise they would be able to harass end-users for their consent and prevent them from providing freely given consent.

Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users that they may contact them, or download a specific application on their terminal equipment, in order to be properly informed about the intended processing and to provide their consent.

Rectial 25

Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages	Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages

to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.	to end-users, for example when they enter stores, with personalized offers. ~~While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations.~~ **In any case, being able to precisely locate individuals is one of the highest form of surveillance. It shall never occur without end-users'consent. Furthermore, service providers shall not even be allowed to use information emitted by terminal equipments in order to request such consent, otherwise they would be able to harass end-users for their consent and prevent them from providing freely given consent.** ~~P~~ **Instead, p**roviders engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users **that they may contact them, or download a specific application on their terminal equipment, in order to be properly informed about the intended processing and to provide their consent.** ~~prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.~~

Justification:

Tracking end-users' device should only be authorised if end-users actively consent to be tracked. Such a consent would not be freely given if providers may be able to automatically send numerous requests to all end-users enterring the monitored area.

Article 9

1.The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.	1.The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.
2.Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.	~~2.Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.~~ **2. Access to a service shall not be denied to an end-user for the sole reason that he or she has refused to give his or her consent to processing which are not strictly necessary for the provision of this service.**
3.End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.	3.End-users who have consented to the processing of electronic communications data as set out in ~~point (c) of A~~rticle 6~~(2) and points (a) and (b) of Article 6(3)~~ shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.

Justification:

Expressing consent through technical settings of a software application enabling access to the internet is equivalent to give it through automated means. It implies to give it before being provided with complete information about the

intended processing and thus before knowing for which purposes data may be collected and processed, for how long, by whom, whether they can be disclosed to third parties, transferred outside the Union, etc. In such cirumstances, end-users can never give informed and valid consent, as defined in article 4(11) of the GDPR. Thus, end-users are not be able to express their consent through automated means and this Regulation should not provide accept it.

Furthermore, this article should clearly specify what a freely given consent means.

Recital 21

Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.	Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in **or emitted by** terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of **remembering the choice of end-users not to give their consent to other processing or for the purpose of** enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. ~~Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website.~~ Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

Recital 22

The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to	The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment **but their choice not to consent is rarely remembered by service providers.** As a result, end-users are overloaded with requests to provide consent. ~~The use of technical means to provide consent, for example, through transparent and user-friendly settings,~~ **Imposing specific and limited obligations on service providers** may address this problem. Therefore, this Regulation should provide for the possibility **for end-users to order service providers to remember their choice not to consent and to stop requesting their consent once they have refused to give it** ~~to express consent by using the appropriate settings of a browser or other application~~. The choices made by end-users ~~when establishing its general privacy settings of a browser or other~~ application should be binding on, and enforceable against, any third parties. **Furthermore,** Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same

prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.	capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

Justification:

Consent is not freely given if end-users who had already refused to give it may be requested to do so over and over again, impeding their use of the service, until they finally give it.

Article 10

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.	1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer **and set by default** the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.

Recital 23

The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in a an easily visible and intelligible manner.	The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies', **which prevents end-users from providing informed and freely given consent, overloading them with requests**. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers **and sets by default** the option to prevent third parties from **requesting end-users' consent to** store~~ing~~ information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never **ask whether to** accept cookies **but always reject them**') to lower (for example, 'always **ask whether to** accept cookies') and intermediate (for example, 'reject third party cookies **without asking**' or 'only **ask whether to** accept first party cookies **and reject other cookies**'). Such privacy settings should be presented in a an easily visible and intelligible manner.

Justification:

End-users should not be able to express their consent through automated means (for example through technical settings of a software application enabling access to the internet) but, in order not to be overloaded with requests, they should be able to automatically reject some categories of request.

Recital 24

For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should,	~~For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should,~~

among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.	~~among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.~~

Justification:

Consent expressed through automated means (for example through technical settings of a software application enabling access to the internet) can never be informed nor valid.

Article 11

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.	1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to ~~safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.~~ **safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as referred to in Article 23(1)(d) of Regulation (EU) 2016/679. For this purpose, Union or Member State law may not impose on electronic communications service providers an obligation to retain electronic communications data related to all of their end-users but may only allow courts to order such providers to retain electronic communictions metadata relating to specifically identified end-users for a duration that cannot exceed two months.** **1a. Electronic communications data may only be accessed by public authorities for safeguarding the prevention, investigation, detection or prosecution of serious crime and with the prior authorisation of**

	a court.

Justification:

Electronic communications service providers are already authorised by this Regulation to store a huge amount of data for security or billing purposes. Thus, Member States hardly ever need to order providers to retain data: they are already stored by the vast majority of providers. However, since some very specific kinds of data may not be actively stored by some provider in very specific circumstances, courts should still be able to request them to do so for a proportionate duration.

Furthermore, access by the public authorities to data retained by providers should be limited to the most important purposes and by the prior authorisation of a court.

Recital 26

When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).	When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard ~~specific public interests, including national security, defence, public security and~~ the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security ~~and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests~~. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above **the fight against serious crimes and if such measures cannot be taken without the prior authorisation of a court** , in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).

Article 23

2.Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:	2.Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a) the obligations of any legal or natural person who process electronic communications data pursuant to	~~(a) the obligations of any legal or natural person who process electronic communications data pursuant to~~

Article 8;	~~Article 8;~~
(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;	(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;
(c) the obligations of the providers of publicly available directories pursuant to Article 15;	(c) the obligations of the providers of publicly available directories pursuant to Article 15;
(d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.	(d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.
3.Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	3.Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, ~~and~~ 7 **and 8** shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Justification

Being able to precisely locate individuals is one of the highest form of surveillance. It shall be limited with the same firmness as other forms of surveillance.