PROPOSAL FOR AMENDMENTS

Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003 (COD)

Committee on Civil Liberties, Justice and Home Affairs (LIBE)

Rapporteur: Marju Lauristin (S&D)

Original Text	**EDRi proposed amendments**
ARTICLE 1	**ARTICLE 1**
CHAPTER I GENERAL PROVISIONS	CHAPTER I GENERAL PROVISIONS
Article 1 Subject matter	Article 1 Subject matter
1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.	1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.
2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, **which shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data.**	2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union. ***Justification: The deleted wording is superfluous.***
3. The provisions of this Regulation particularise	3. The provisions of this Regulation particularise

and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.	and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2. The rules and provisions in Regulation (EU) 2016/679 will continue to fully apply to the processing of personal data subject to this Regulation in relation to any activity not specifically regulated by this instrument. **4. Where the specific rules in paragraph 3 involve processing of personal data that are subject to Regulation 2016/679, both Regulations apply. In cases of conflict between the two Regulations, the EDPB shall determine the instrument that should apply.** **5. In coming to a determination in line with Paragraph 4, the EDBP shall consider that the interests for natural persons are paramount.** ***Justification: This will help minimise confusion due to the scope of the term "end user" in the Commission's proposal***

Original Text **Relevant Recitals - Article 1**	**EDRi proposed amendments**
RECITALS 1-6	**RECITALS 1-6**
(1) Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the parties **involved in a communication.** The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e mail, internet phone calls and **personal** messaging provided through social media.	(1) Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication**s**, including **information regarding** when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the **communicating** parties. The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e mail, internet phone calls and messaging provided through social media.
(2) **The content of** electronic communications	(2) Electronic communications may reveal highly

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.	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 protection of confidentiality of communications is an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, freedom of assembly, freedom of expression and information.** ***Justification: This serves to underline the importance of the instrument.***
(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council 4 , also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.	(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that **certain** provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council, also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679 When reference is made to consent by an end-user, including legal persons, the definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.

(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.	
(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 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.	(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 **can**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**, and on a legal ground specifically provided under,** this Regulation.
(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of online behaviour of end-users, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.	

Original Text	**EDRi proposed amendments**
ARTICLE 2	**ARTICLE 2**
Article 2	Article 2

Material Scope 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. 2. This Regulation does not apply to: (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; (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; 3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001]. 4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC 9 , in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. 5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.	Material Scope 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 **regardless of whethe a payment is required by the user**. **(e) (new) hardware and software placed on the market permitting electronic communications between users or end-users, including the trieval and presentation of information on the Internet;**

Original Text	EDRi proposed amendments
Relevant Recitals-Article 2	
RECITALS 7-8	**RECITALS 7-8**
(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.	***(7)*** **[deleted]** ***Justification: The first part of recital 7 would undermine the clarity of the proposal. The second sentence suggests a balance should be made between something that is a fundamental right and something that is not a fundamental right.***
(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.	8) This Regulation **sets forth rules that** 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. ***Justification: Linguistic edit.***

Original Text	EDRi proposed amendments
ARTICLE 3	**ARTICLE 3**
Article 3 Territorial scope and representative 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; (b) the use of such services; (c) the protection of information related to the	(c) the protection of information related to the

terminal equipment of end-users **located** in the Union. 2. Where the provider of an electronic communications service is not established in the Union it shall designate in writing a representative in the Union. 3. The representative shall be established in one of the Member States where the end- users of such electronic communications services are located.	terminal equipment of end-users in the Union. ***Justification: This improves predictability of scope.*** **Article 3*bis*** **Applicable law in the online environment** **1. To the extent that Regulation (EU) 2016/679 or this Regulation allows Member States to regulate the processing of personal data or electronic communications data, in their domestic laws, the relevant national law provisions shall apply to:** **(a) the processing of personal data or electronic communications data in the context of the activities of an establishment of a controller, processor or a provider of an electronic communications service or network established in the Member State in question; or** **(b) the processing of personal data or electronic communications data by a controller, processor or a provider of an electronic communications service or network not established in the Union , offering goods or services in that Member State or monitoring the behaviour of data subjects in that Member State;** **2. The relevant national law provisions as set out in point 1 of this Article do not apply to the processing of personal data or electronic communications data in the context of the activities of an establishment of a controller, processor or a provider of an electronic communications service or network established in another Member State, who shall instead only be subject to the relevant national law provisions of that other Member State.** *Justification: This addresses legal doubts regarding the place of establishment rule for providers/controllers and rules when they are not established in the Union.*

4. The representative shall **have the power** to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.	4. The representative shall **be authorised by the provider** to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, **courts** and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation **and shall be provided with any relevant information to that end by the provider, to the extent that the provider does not answer the questions or provide the information directly.** ***Justification: This clarifies the scope of the powers of the representative***
5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against a natural or legal person who processes electronic communications data in connection with the provision of electronic communications services from outside the Union to end-users in the Union.	
EDRi comments:	

Original Text **Relevant Recitals-Article**	EDRi proposed amendments
RECITAL 9	**RECITAL 9**
(9) This Regulation should apply to electronic communications data processed in connection with the provision and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to	**No Amendment**

end-users in the Union.	

Original Text	**EDRi proposed amendments**
ARTICLE 4	**ARTICLE 4**
Article 4 Definitions 1. For the purposes of this Regulation, following definitions shall apply: (a) the definitions in Regulation (EU) 2016/679; (b) the definitions of ‘electronic communications network’, ‘electronic communications service’, ‘interpersonal communications service’, ‘number-based interpersonal communications service’, ‘number-independent interpersonal communications service’, ‘end-user’ and ‘call’ in points (1), (4), (5), (6), (7), (14) and (21) respectively of Article 2 of [Directive establishing the European Electronic Communications Code];	Article 4 Definitions 1. For the purposes of this Regulation, following definitions shall apply: (a) the definitions in Regulation (EU) 2016/679; (b) ‘electronic communications network’ **means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;** (c) ‘electronic communications service’ **means a service normally provided for remuneration via electronic communications networks, which encompasses 'internet access service' as defined in Article 2(2) of Regulation (EU) 2015/2120; and/or 'interpersonal communications service'; and/or services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;** *Justification: The concept of “editorial control” is becoming too unclear in the EU legal framework (see copyright Directive, AVMS Directive, etc). This part of the EECC definition has therefore been removed.* (d) 'interpersonal communications service’ **means a service normally provided for remuneration that**

	enables direct interpersonal and interactive exchange of information via electronic communications networks. This includes services that enable interpersonal and interactive communication as a minor ancillary feature that is intrinsically linked to another service. (e) 'number-based interpersonal communications service' **means an interpersonal communications service which, uses assigned numbering resources, i.e. a number or numbers in national or international telephone numbering plans partly or fully as its addressing system;** ***Justification: Some services sometimes use numbering to interconnect with the PSTN and sometimes and sometimes use the same numbering to terminate calls without using the PSTN. This amendment seeks to achieve a more technologically neutral outcome.*** (f) 'number-independent interpersonal communications service' **means an interpersonal communications service which does not connect with the public switched telephone network, either by means of assigned numbering resources, i.e. a number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;** ***(g) 'user' or*** 'end-user' **means a natural person using a publicly available electronic communications service, without necessarily having subscribed to this service;** **(h) 'call' means a connection established by means of a publicly available electronic interpersonal communications service allowing voice communication between two or more end-points;** **(i)** the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC 10 .
(c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC 10 .	**(j) (new) "normally for remuneration" means involving an economic transaction, whether financial or not**

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.	
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 **or via electronic communications networks,** such as text, voice, videos, images, and sound; ***Justification: Brings the text back into line with its clearer, pre-publication version.***
(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 generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;	c) 'electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including**, but not limited to,** data used to trace and identify the 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; **It includes data broadcast or emitted by the terminal equipment to identify end-users' communications and/or terminal equipment in the network and enable it to connect to such network or to another device.** ***Justification: As also suggested by WP29 and by the EDPS, the reference to the proposed EECC should be removed and include the definitions in proposed ePrivacy Regulation instead. First,***

	because both legislative acts are still in a draft form and this could lead to changes on the proposed terms. Second, because it will be difficult for the legislators to coordinate and work simultaneously on both legislative proposals. Last, the definitions, as they are proposed at the moment already present differences between the two pieces of legislation.
(d) 'publicly available directory' means a directory of end-users of electronic communications services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service;	(d) 'publicly available directory' means a directory of end-users of electronic communications services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service;
(e) 'electronic mail' means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;	(e) 'electronic mail' means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;
(f) 'direct marketing communications' means any form of advertising, **whether written or oral,** sent, to one or more identified or identifiable end-users **of electronic communications services,** including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;	(f) 'direct marketing communications' means any form of advertising **or similar promotion,** ~~–~~ sent, **directed or presented** to one or more identified or identifiable end-users **over an electronic communications network**, including the use of automated calling and communication systems with or without human interaction, **targeted advertising on social media platforms**, electronic mail, **facsimile**, SMS, etc.; *Justification: This brings the text into line with technological realities*
(g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems;	(g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems**, and which connect the caller and the recipient of the call with or without the use of semi-automated communication systems, such as for example automatic dialers**; **Justification: In line with WP29 opinion**

(h) ‘automated calling and communication systems’ means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, **including calls made using automated calling and communication systems which connect the called person to an individual**.	(h) ‘automated calling and communication systems’ means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech.- **i) new ‘equipment location data’ means data that can enable the geospatial location, movement or direction of terminal equipment and it is not processed in order to provide a communications service.**

Original Text **Relevant Recitals - Article 4**	**EDRi proposed amendments**
RECITALS 10-14	
(10) Radio equipment and its software which is placed on the internal market in the Union, must comply with Directive 2014/53/EU of the European Parliament and of the Council . This Regulation should not affect the applicability of any of the requirements of Directive 2014/53/EU nor the power of the Commission to adopt delegated acts pursuant to Directive 2014/53/EU requiring that specific categories or classes of radio equipment incorporate safeguards to ensure that personal data and privacy of end-users are protected.	**No amendment**
(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. In order to ensure an effective and equal protection of end- users when using functionally equivalent services, this Regulation uses the definition of electronic communications services set forth in the [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code 7]. That definition encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services.	(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. In order to ensure an effective and equal protection of end-users when using functionally equivalent services, this Regulation uses the definition of electronic communications services set forth in the [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code 7]. That definition encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services.

The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.	The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service, **such as internal messaging, newsfeeds, timelines and similar functions in online services where messages are exchanged with other users within or outside that service (ie: public and privately available newsfeeds and timelines)**; therefore, such type of services also having a communication functionality should be covered by this Regulation. ***Justification: This ensures that ancillary services are not downgraded by the regulation, as suggested by the EC in its presentation of the new legislation*** (new recital 11.bis): **The definition of "end-user" includes for instance employees, tenants, hotel guests, family members, visitors, and any other individuals who are as a matter of fact using the services, for private or business purposes, without necessarily having subscribed to it**.
(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.	
(13) The development of fast and efficient wireless technologies has fostered the increasing availability	(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.	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, **airports, hotels, hostels,** hospitals **and other similar Internet access points.** 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.
(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.	(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. **It should also include location data, such as for example, the actual or inferred location of the terminal equipment, the location of the terminal equipment from or to which a phone call or an internet connection has been made, or the Wi-Fi hotspot that a device is connected to, as well as data necessary to identify end-users' terminal equipment.** 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. **14a) (new) Equipment location data should include data transmitted or stored in terminal equipment generated by accelerometers, barometers, compasses, satellite positioning systems or similar sensors or devices.**

Original Text	**EDRi proposed amendments**
ARTICLE 5	**ARTICLE 5**
CHAPTER II PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT Article 5 Confidentiality of electronic communications data Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	CHAPTER II PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT Article 5 Confidentiality of electronic communications data Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance**,** or **any** processing of electronic communications data **regardless of whether this data is in transit or stored**, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation. ***Justification: Addition of "any" ensures consistency with GDPR.*** **2. Neither providers of electronic communication services, nor any third parties, shall process electronic communications data that are not collected on the basis of consent or any other legal ground under this Regulation, or any other legal basis not specifically provided for in this Regulation**

	Justification: In line with EDPS opinion ,this will clarifty that any further data processing cannot rely on grounds other than those contained in the ePrivacy Regulation.
EDRi comments:	

Original Text **Relevant Recital – Article 5**	**EDRi proposed amendments**
RECITAL 15	**RECITAL 15**
(15) **Electronic communications data should be treated as confidential. This means that a**ny 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.	(15) **Any processing of electronic communications data or** any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, **by persons other than the end-users,** should be prohibited. **When the processing is allowed under any exception to the prohibitions under the this Regulation, any other processing of the electronic communications data on the basis of Article 6 of the Regulation (EU) 2016/679 shall be considered as prohibited, including processing for another purpose on the basis of Article 6(4) of that Regulation. This would not prevent controllers from asking for additional consent for new processing operations.** The prohibition of interception of communications data should apply **also** during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee **and any temporary files in the network after receipt**. 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**, and**

	analysis of end users' electronic communications metadata, including browsing habits without the end-users' consent. ***Justification: Clarifications of the text and re-inserting earlier positive wording from Commission***

Original Text	EDRi proposed amendments
ARTICLE 6	**ARTICLE 6**
Article 6 **Permitted** processing of electronic communications data 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 (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.	Article 6 **Lawful** processing of electronic communications data 1. Providers of electronic communications networks and services may process electronic communications data, if: (a) it is **strictly** necessary to achieve the transmission of the communication, for the duration necessary for that purpose **only**; or (b) it is **strictly** 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 **only and only to the extent that the purpose concerned could not be fulfilled by processing information that is made anonymous;** **(c) Where processing of electronic communications data in accordance with point (b) of Article 6 (1) is likely to result in a high risk to the rights and freedoms of natural persons, Articles 35 and 36 of Regulation (EU) 2016/679 shall apply.** **(d) Under no circumstances, including when complying with points (a) and (b) of Article 6 (1), shall providers of electronic communications services try to, be requested to or be forced to comply with a request to, gain access to end-user's communications content in situations where the content itself is protected by technical means..** 2. Providers of electronic communications services may process elctronic communications metadata **only** if: (a) it is **strictly** necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic

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 11 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 (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.	Communications Code] or Regulation (EU) 2015/2120 11 for the duration necessary for that purpose; or (b) it is **strictly** necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, **unlawful** use of, or subscription to, electronic communications services; or (c**) after receiving all relevant information about the intended processing in a clear and easily understandable language, provided separately from the terms and conditions of the provider,** 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 **all** end-users **, or which are provided in order to deliver a specific functionality to the end-user concerned**, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous. **(e) Where a type of processing of electronic communications metadata (and taking into account the nature, scope, context and purpose of processing) is likely to result in a high risk to the rights and freedoms of natural persons, Articles 35 and 36 of the GDPR shall apply.** **Consent may be provided to the provider of the communication service or to the provider of the specific service, but if it is provided to the latter, the latter must be able to prove to the provider of the communication service that such consent has been given.** **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; (***(b) In cases covered by point (a) of Article 6 (3), ,*** the provider ***shall*** consult the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.
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 (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** consult**ed** the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.	

Original Text	**EDRi proposed amendments**
Relevant Recitals - Article 6	
RECITALS 16, 17, 19	**RECITALS 16, 17, 19**
(16) The prohibition of storage of communications	(16) The prohibition of storage of communications

is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications network. It should not prohibit either the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including checking security threats such as the presence of malware or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc.	is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications network. It should not prohibit either the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including checking security threats such as the presence of malware or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc. **Where a type of processing of electronic communications data for these purposes 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.**
(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 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**	(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 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, **but rather, equipment location data'. In any case, location data of the terminal device of a natural person is personal data and thus the processing of those data is subject to the obligations from the Regulation (EU) 2016/679.** Examples of commercial usages of electronic communications metadata by providers of electronic

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 services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. 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, **providers must comply with the obligations from Article 25 GDPR in case of further processing of location data or other metadata, conduct** 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. **Moreover, the parties involved in the processing of location data and other metadata should make public their methods of anonymisation and further aggregation, without prejudice to secrecy safeguarded by law**. **The anonymisation method must, once the defined purposes of processing have been fulfilled, technically prevent all parties from singling out an end-user within a set of data or from linking new data collected from the end-user's device to the existing set of data.**
(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	(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**

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.	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. **In exceptional circumstances, communications service providers may provide the means for additional processing of electronic communications data with the consent of one of the parties to a communication, on condition that this processing is for the provision of services requested by that party and that this is strictly necessary for delivering a specific functionality, in particular such services such as voice-to-text or other automatic content processing used as accessibility tools needed by persons with disabilities. Third parties providing the means for recording, storing or otherwise processing such data used by end-users in the course of a purely individual household or individual activity, as long as this activity is part of the strictly functional aspect of hardware and software which the end-user can reasonably expect (such as voice-to- text technology, or spell checkers), shall process such data in accordance with Regulation (EU) 2016/679.** 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. ***Justification:***

	The creation of heat-maps does not require linking the positions of individual end-users. Heatmaps are already created in practice by aggregating the number of end-users in each network cell and by comparing the changes on a per-cell basis instead of using end-user identifying data. This a real-world example of privacy-by-design through the use of truly anonymous data by innovative startups like mezuro.com.

Original Text	**EDRi proposed amendments**
ARTICLE 7	**ARTICLE 7**
Article 7 Storage and erasure of electronic communications data 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. 3. Where the processing of electronic communications **meta**data takes place for the purpose of billing in accordance with point (b) of Article 6(2), the **relevant meta**data may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.	Article 7 Storage and erasure of electronic communications data 1. Without prejudice to point (b) of Article 6(1)**,** points (a) and (**c**) of Article 6(**2**) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications **data** or make that data anonymous **when it is no longer strictly necessary for the exchange of the communications.** 3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the **strictly necessary** data may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law. ***Justification*** ***There is no justification to treat the confidentiality***

	of metadata and content differently. Both these categories of communications data are highly sensitive data needing sufficient protection. Furthermore, the distinction between content and metadata is often not clear-cut, which also calls for similar protection and a similar regulatory regime. ***The current language appears to limit the protection of communications data to data in transit only. The conceptual framework of this distinction between communications 'in transit' and 'stored' communications is outdated. With the popularity of cloud-based services, most communications data currently remain stored with service providers, even after receipt by the intended addressee. The confidentiality of communications data should remain protected as long as the service provider has control over this data.***

Original Text **Article**	**EDRi proposed amendments**
ARTICLE 8	
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: (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	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 **information** about its software and hardware **and any other electronic communications data identifying end-users**, other than by the end-user concerned**,** shall be prohibited, except on the following grounds: ***Justification: To cover all relevant processing*** (a) it is **strictly** necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) **all** end-user**s have** given **their** consent; or *Justification: As per EDPS opinion, consent needs to cover all parties of the communications. This amendment seeks to achieve that.*

(c) it is necessary for providing an information society service requested by the end-user; or	(c) it is **strictly** necessary for providing an information society service requested by the end-user; or ***Justification: As per WP29 Opinion. This exception applies if strictly necessary in order to obtain information about the technical quality or effectiveness of a delivered information society service and had no or little impact on the privacy of the subscriber or end user involved.***
(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 **strictly** necessary ***for the measurement of use of* the information society service requested**, provided that such measurement **does not entail tracking of the end-user across different information society services, the data is anonymised, and that this measurement** is carried out **directly under the responsibility of** the provider of the information society service requested by the end-user. **(e) The end-user shall not be denied access to an information society service or electronic communications service (whether these services are remunerated or not) on grounds that the end-user does not provide consent under point (b) of Article 8(1) or point (b) of Article 8(2) for processing any data that is not strictly necessary for the provision of that service.** ***Justification: As per the EDPS opinion and in line with the requirement of freely given consent, particularly as it will apply to all devices, including IoTs.*** **(f) The end-user shall not be denied any functionality of the terminal equipment on grounds that the end-user does not provide consent as set out in point (b) of Article 8(1) or point (b) of Article 8(2) for processing any data that is not strictly necessary for the functionality requested by the end-user.**

	Justification: Brings the text into line with the EDPS opinion and in line with the requirement of freely given consent, particularly as it will apply to all devices, including IoTs.
	Justification: **Ban on tracking walls** ***It is not justified to require users to agree to an unlimited "take it or leave it" amount of unnecessary processing of their personal data. Electronic communications services (such as broadband internet access and voice communications), information society services (such as websites and apps), and 'smart devices' (e.g. smart cars, smart TVs, etc.) are increasingly essential for individuals to be able to communicate and participate in our society. Providers of these services and suppliers of these smart devices often force individuals to consent to data processing activities unnecessary for the provision of the service itself or for the normal functionality of the smart device. Individuals often have no genuine and free choice, or are unable to refuse or withdraw consent without detriment. Such take it or leave it options or "tracking walls" leave people with no choice than to accept the processing of their personal data.*** ***The proposed text clarifies and particularises the conditions of consent under Article 7(4), and Recitals (42) and (43) of the GDPR to the context of the electronic communications sector and the Internet of Things. It ensures that consent will be genuinely freely given and that individuals have access to electronic communications services, websites, apps, and the functionality of smart devices, without being subject to invasive processing practices.***
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 shall be prohibited, except if: ***Justification: Data is emitted even if a connection does not take place.***
	(a) it is done exclusively in order to, for the time

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or	necessary for, and for the purpose of establishing a connection**, which all end-users have authorised**; or ***Justification: In line with EDPS opinion, this aims to ensure that all affected end-users are protected.***
(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**. T**he 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.	**(**b**) all relevant information about the intended processing is provided in clear and easily understandable language, provided separately from the terms and conditions of the provider, and if the end-user concerned has given his or her consent to the processing of the data for one or more specified purposes, including for the provision of specific services, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous; t**he 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 **and supplemented with a mandatory data protection impact assessment**, have been applied. ***Justification: This brings the proposal into line with the approach in the rest of the legislation***
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. [deleted]** ***Justification: no longer needed.***
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 [deleted]** **Justification: no longer needed.**

Original Text Relevant Recitals – Article 8	EDRi proposed amendments
RECITALS 20, 21, 25	**RECITALS 20, 21, 25**
(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes.	(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities,including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities **or to instigate certain technical operations or tasks, often without the knowledge of the user**. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. **A high and equal level of protection of the private sphere of users needs to be ensured in relation to the privacy and confidentiality of users' terminal equipment content, functioning and use.** Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific, **limited,** and

	transparent purposes.
(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.**	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 **by the person or legal person in charge of the website ("first party analytics")**. **21(b) Equipment location data can give a very detailed and intrusive insight on an individual's personal life or an organisation's business and activities. Processing of location data from any source, whether electronic communications metadata or equipment location data should be conducted on the basis of clear rules.**
(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,	(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to 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.	providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information **is often** used for more intrusive purposes, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers. **Such practices should be prevented to ensure compliance with the principle of purpose limitation as defined under Regulation (EU) 2016/679.** 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.**. Therefore, only in a limited number of circumstances and only if the used data would be anonymised or deleted after the defined purposes of processing have been fulfilled, might data controllers be allowed to process the information emitted by the terminal equipment for the purposes of tracking end-users physical movements with his or her consent. The anonymisation method must technically prevent all parties from singling out an end-user within a set of data or from linking new data collected from the end-user's terminal equipment to the existing set of data.** Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.

Original Text	**EDRi proposed amendments**
ARTICLE 9	**ARTICLE 9**
Article 9 Consent 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.**	Article 9 Consent 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. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) points (a) and (b) of Article 6(3), point (b) of Article 8(1) and point (b) of Article 8(2) 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 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. In order to lower the burden on end-users, requests for consent as well as consent withdrawals shall where possible conform to technical standards applicable to such request or withdrawals and be machine-readable, in order to allow for end-users to benefit from privacy-enhancing-technologies.** ***Justification*** ***<u>No generic consent through browser settings</u>*** ***Consent under point (2) of Article 9 cannot meaningfully be informed consent within the meaning of the GDPR. Therefore, the proposed language under point (2) should be deleted. The current language incorrectly suggests that valid consent can be given through non-specific browser settings.*** ***Browsers can currently only give general information on the catch-all level that (third party) cookies can be used for tracking. Standards that allow for more fine-grained control are in development but are not widely accepted yet. Also, there is no generic way to technically block device fingerprinting in the browser since there are so many different ways of carrying out device fingerprinting. Moving the handling of consent for cookies to the browser may makes choices for end-users more confusing.*** ***End-users should always remain able to give separate consent per website, app, device, etc. for tracking purposes. From this it follows that for end-users to give meaningful consent they should be provided with a sufficient level of information in a non-intrusive manner. In order to allow browsers and other user agents to support the end-users in this in the least intrusive fashion possible (no cookie banners), it is necessary that the information provided by online services relevant to the consent decision is presented in a machine-readable format.*** ***<u>Reminder consent withdrawal</u>*** ***Art. 9(3) requires that end-users are reminded (every six months) of their possibility to withdraw their consent at any time. This only applies to consent for the analysis of metadata and content. It should be clarified that this obligations also applies to consent in the context of interference with terminal equipment and device tracking as***

	stipulated in Article 8.

Original Text **Relevant Recitals- Article 9**	**EDRi proposed amendments**
RECITALS 18, 22, 24	**RECITALS 18, 22, 24**
(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 unable to refuse or withdraw consent without detriment.	(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 **with remuneration paid by a third party rather than by the recipient of the service .** 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. **Individuals depend on and financially contribute (through taxes) to public services, services that are financed directly, indirectly, totally or partially by public funds such as medical services that are essential to fully participate in a democratic society. These services ensure and strengthen the enjoyment of human rights. Without access to these services individuals cannot fully participate in their societies . Therefore, preventing access to such services unless consent is provided to processing activities that are not strictly required for the performance of these services, must be prohibited. In addition to this, b**asic broadband internet access, voice communications services, **and other electronic communications services that have or have the potential to be used widely,** are **in today's' societies** essential services that allow individuals to communicate and participate in increasingly more aspects of their lives. 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. **Also, the growing use and dependence of so-called 'smart' devices, such as smart cars, smart phones and smart TVs, are increasingly essential devices for individuals to participate in our 'connected' society. Individuals often have no genuine and free choice when accessing those essential services or using those smart devices because they are**

	unable to refuse or withdraw consent without detriment to themselves. Situations where the individual is confronted with "take it or leave it" options, for example when they face "tracking walls", leave them *without* a real choice. Access to these essential services or the functionality of terminal equipment should not depend on the requirement of consent to the processing of data that is not strictly necessary for the services or for the functionality requested. Intrusive processing activities, such as analysing electronic communications content, electronic communications metadata, or tracking user activity over time or across several information society services or terminal equipment, for purposes such as providing targeted advertisements cannot be considered as strictly necessary for the service or functionality requested. ***Justification: For the justification of the suggested changes, see the justification under Article 8 .***
(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.**	(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. Communications software should be set **by default to the most privacy friendly option**. The choices made by **all** end-users when establishing **their** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are **one of the ways to access and send** information on the internet. Other types of application, such as the ones that permit calling and messaging or provide route guidance, have **similar** capabilities.

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.	
(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, 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.	**24. [delete]**
EDRi comments	

Original Text	**EDRi proposed amendments**
ARTICLE 10	**ARTICLE 10**
Article 10	Article 10

Information and options for privacy **settings to be provided**	**P**rivacy **by design and by default**
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. **The settings of all the components of the terminal equipment placed on the market, including both software and hardware, shall be configured by default to prevent third parties from storing information, processing information already stored in the terminal equipment and preventing the use by third parties of the equipment's processing capabilities.** **1(a).** Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall **be configured by default** to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.
2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.	**2.** ***[deleted]***
3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.	**2**. In the case of software which has already been installed on 25 May 2018, **and which has not been officially discontinued by that date with a public announcement from the software provider,** the requirements under paragraphs 1 and **1(a)** shall be complied with at the time of the first update of the software, and, in any case no later than 25 August 2018.
EDRi comments:	

Original Text Relevant Recitals	EDRi proposed amendments
RECITAL 23	
(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.	(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 **trackers**. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept **trackers**') to lower (for example, 'always accept **trackers**') and intermediate (for example, 'reject third party **trackers** ' or 'only accept first party **trackers**'). Such privacy settings should be presented in a an easily visible and intelligible manner. **For web browsers and any other software enabling access to the internet or internet-based services to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking, they should, among others, require a clear affirmative action from the end-user of terminal equipment to express his or her freely given, specific, informed and explicit agreement to the storage and access of 'cookies' or any other trackers in and from the terminal equipment. 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. That information provided to the users shall not be written in a way that seeks to dissuade end-users from selecting the most privacy-friendly settings and should include relevant information about the risks associated to allowing third party trackers to be stored in the device, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising or sharing that information with third parties. 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 white-list certain websites or to specify for which websites (third) party trackers are always or never allowed. In case of no active choice, or action from the user, web browsers and any other software enabling access to internet-based services shall be set by default to ensure the highest degree of protection for the individual, including the rejection and blocking the storage of third party 'cookies' or other type of trackers.

Original Text	EDRi proposed amendments
ARTICLE 11	**ARTICLE 11**
Article 11 Restrictions 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) o Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests**.	Article 11 Restrictions 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 **is limited to a range of targets based on reasonable suspicion,** respects the essence of the fundamental rights and freedoms**,** and is a necessary appropriate and proportionate measure in a democratic society to safeguard **national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of serious criminal offences or unauthorised use of electronic communication systems, and the request is done following a prior judicial authorisation.** ***Justification:*** ***First, as regards the limits on the implementation of national data retention law, after Tele2/Watson decision, it is clear that retention frameworks providing for anything other than targeted retention are not allowed under the Charter. The Court[1] made it very clear that any legislation that does not limit the range of targets based on reasonable suspicion is unlawful, because it amounts to a violation of the principles of strict necessity and proportionality.*** ***Second, the reference to Article 23 (1)(a)-(e), undesirably broadens the possibilities to retain data, therefore, it is better to keep the purposes mentioned in Article 15 of the ePrivacy Directive.*** **2. Notwithstanding the restrictions of paragraph 1, Member States shall not impose any obligations on the provider of an electronic communications network or service that would result in the weakening of the security and encryption of their networks and services."** **Justification** **The weakening of the security and encryption of electronic communications networks and services, would compromise the security and**

1 CJEU Joined Cases C-203/15 and C-698/15 TELE2, Watson et al.

	integrity of the electronic communications infrastructure, which could have grave consequences for citizens, governments companies, and the proper functioning of our society. Therefore, obligations imposed by Member States to obtain lawful access to electronic communications data should not include any obligations for providers that would result in the weakening of the security and encryption of electronic communications networks and services.
2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide **the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.**	3. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1.They shall **keep detailed and secure records, in relation to all requests received, of:** **- the in-house staff members who handled requests;** **- the identity of the official or body asking for the information;** **- the purpose for which the information was sought;** **- the date and time of the request;** **- the formal basis and authority for the request, including the identity and status or function of the official who authorised the making of the request and whether this was a judicial or prosecuting or state security official;** **- the number of subscribers to whose data the request related;** **- the precise data provided to the requesting official or body;** **- the period covered by the data;** **and any other information as may be set out in further guidance to be issued by the EDPB.** **The providers shall provide the competent supervisory authority, on demand, with all the above information about any specific request.** **The providers shall also provide the competent authority with regular overall information, at least on an annual basis, on all the requests in a specified period, with such statistical breakdowns as the authority may request.** **The competent authority shall release a meaningful summary of the regular overall information which, on the one hand, shall allow data subjects and the general public meaningful**

	insight into the scope and nature of the use of the powers of access by the relevant authorities, while at the same time protecting confidential information to the extent that that is strictly necessary to safeguards the matters listed in paragraph 1. **4. Direct means of access into the technical facilities of the providers of communication services or communication networks (“back doors”), for the use of the agencies involved in the matters listed in paragraph 1, shall be prohibited.**

Original Text Relevant Recital- Article 11	EDRi proposed amendments
RECITAL 26	**RECITAL 26**
(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).	(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 **(ie: State security)**, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. 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. **Encryption and other security measures are critical to ensure the confidentiality and integrity of electronic communications and the security and integrity of the electronic communications infrastructure as a whole. The measures taken by Member States shall not entail any obligations for the provider of the electronic communications network or service that would result in the weakening of the security and encryption of their networks and services.** 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). **(26a) new The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the end-users of electronic communications services. The**

	availability of electronic communication service options with alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example unregistered SIM cards and facilities for payment by credit card, can mitigate these risks. When the end-user is a natural person who is different from the subscriber receiving the itemised bill, for example in an employment context, the operator of number-based interpersonal communication services should offer their subscribers a different type of itemised bill in which a certain number of digits of the called number have will not be shown. ***Justification: recital 33 in the current e-Privacy Directive 2002/58. The provider of the number-based interpersonal communication service must keep detailed records of the individuals calls in order to provide itemised bills. If the bill is paid by someone else than the natural person making the calls, there is a high privacy risk for the natural person.***

Original Text	**EDRi proposed amendments**
ARTICLE 12	**ARTICLE 12**
CHAPTER III NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS Article 12 Presentation and restriction of calling and connected line identification 1. Where presentation of the calling and connected line identification is offered in accordance with Article [107] of the [Directive establishing the European Electronic Communication Code], the providers of publicly available number-based interpersonal communications services shall provide the following: (a) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis;	**No amendments proposed**

(b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls; (c) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user; (d) the called end-user with the possibility of preventing the presentation of the connected line identification to the calling end-user. 2. The possibilities referred to in points (a), (b), (c) and (d) of paragraph 1 shall be provided to end-users by simple means and free of charge. 3. Point (a) of paragraph 1 shall also apply with regard to calls to third countries originating in the Union. Points (b), (c) and (d) of paragraph 1 shall also apply to incoming calls originating in third countries. 4. Where presentation of calling or connected line identification is offered, providers of publicly available number-based interpersonal communications services shall provide information to the public regarding the options set out in points (a), (b), (c) and (d) of paragraph 1.	

Original Text **Relevant Recital – Article 12**	**EDRi proposed amendments**
RECITAL 27	
(27) As regards calling line identification, it is necessary to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. Certain end-users, in particular help lines, and similar organisations, have an interest in guaranteeing the anonymity of their callers. As regards connected line identification, it is necessary to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected.	**No amendments proposed**

Original Text	EDRi proposed amendments
ARTICLE 13	**ARTICLE 13**
Article 13 Exceptions to presentation and restriction of calling and connected line identification 1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of metadata, on a per- line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications. 2. Member States shall establish more specific provisions with regard to the establishment of procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of malicious or nuisance calls.	**No amendments proposed**

Original Text **Relevant Recital – Article 13**	EDRi proposed amendments
RECITAL 28	**RECITAL 28**
(28) There is justification for overriding the elimination of calling line identification presentation in specific cases. End-users' rights to privacy with regard to calling line identification should be restricted where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services, such as eCall, to carry out their tasks as effectively as possible.	**No amendments proposed**

Original Text	EDRi proposed amendments
ARTICLE 14	**ARTICLE 14**
Article 14 Incoming call blocking Providers of publicly available number-based	Article 14 Incoming call blocking Providers of publicly available number-based

interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge: (a) to block incoming calls from specific numbers or from anonymous sources; (b) to **stop** automatic call forwarding by a third party to the end-user's terminal equipment.	interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge: (a) to block incoming calls from specific numbers **or having a specific code/prefix identifying the fact that the call is a marketing call, as foreseen in Article 16(3)(b),** or from sources blocking calling line ID or equivalent services; ***Justification: EDPS opinion*** (b) to **ensure that** automatic call forwarding by a third party to the end-user's terminal equipment **can only be initiated with the end-user's consent**. ***Justification: WP29 opinion.***

Original Text **Relevant Recital – Article 14**	**EDRi proposed amendments**
RECITAL 29	**RECITAL 29**
(29) Technology exists that enables providers of electronic communications services to limit the reception of unwanted calls by end-users in different ways, including blocking silent calls and other fraudulent and nuisance calls. Providers of publicly available number-based interpersonal communications services should deploy this technology and protect end-users against nuisance calls and free of charge. Providers should ensure that end-users are aware of the existence of such functionalities, for instance, by publicising the fact on their webpage.	**No amendments proposed**

Original Text	**EDRi proposed amendments**
ARTICLE 15	**ARTICLE 15**
Article 15 Publicly available directories 1. The providers of publicly available **directories** shall obtain the consent of end-users who are natural persons to include their personal data in **the** director**y** and, consequently, shall obtain consent from these end-users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory **as**	Article 15 Publicly available directories 1. The providers of publicly available electronic **communication services** shall obtain the consent of end-users who are natural persons to include their personal data in director**ies** and, consequently, shall obtain consent from these end-users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the

determined by the provider of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.	directory. Providers shall give end- users who are natural persons the means to verify, correct and delete such data. ***Justification: only the provider of the electronic communication service is in a position to obtain consent from the end-user.***
2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.	2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to **different categories of** their own data. **A separate consent shall be required for enabling reverse searches of natural persons based on phone numbers or service identifiers such as email addresses or user names.** *Justification: EDPS and WP29 opinion.*
3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.	3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.
4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.	4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.

Original Text	**EDRi proposed amendments**
Relevant Recitals – Article 15	
RECITALS 30-31	

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person requires that end-users that are natural persons are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.	
(31) If end-users that are natural persons give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, providers of publicly available directories should inform the end-users of the purposes of the directory and of the search functions of the directory before including them in that directory. End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the end-user's contact details can be searched should not necessarily be the same.	(31) If end-users that are natural persons give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, providers of publicly available directories should inform the end-users of the purposes of the directory and of the search functions of the directory before including them in that directory. End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the end-user's contact details can be searched should not necessarily be the same. **Since reverse searches of natural persons based on phone numbers or service identifiers such as email addresses or user names may be regarded as more intrusive than other searches, a separate consent should always be required before enabling such searches of the end-user.** ***Justification: . In line with WP29 opinion. Provides clarity that separate consent is required for reverse searches which are more intrusive to privacy.***

Original Text	**EDRi proposed amendments**
ARTICLE 16	**ARTICLE 16**
Article 16	Article 16

Unsolicited communications 1. Natural or legal persons **may use** electronic communications **services** for the purposes of sending direct marketing communications to end-users who are natural persons **that** have given their consent.	Unsolicited communications 1. **The use by n**atural or legal persons **of** electronic communications **networks** for the purposes of sending**, directing or presenting** direct marketing communications to end-users who are natural persons **may be allowed only in respect of end-users who** have given their **prior** consent. *Justification: In line with WP29 opinion. There should be a prohibition on sending direct marketing to natural persons without prior consent. Furthermore, it's important that the definition of direct marketing is up-to-date with today's technological realities where direct marketing messages are presented (targeted) to citizens in a number of ways.*
2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.	2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services **for a period of no more than 12 months** only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent. *Justification: WP29 recommends that a time limit is put on the implied consent.*
3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall: (a) present the identity of a line on which they can be contacted; **or** (b) present a specific code/or prefix identifying the fact that the call is a marketing call. 4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not	3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall: (a) present the identity of a line on which they can be contacted; **and** (b) present a specific code/or prefix identifying the fact that the call is a marketing call. *Justification: WP29 and EDPS opinion.* 4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct

expressed their objection to receiving those communications.	marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications. **Member States availing of this exception shall establish a national "Do Not Call" register and provide by law that end-users who are natural persons can object to all future direct marketing voice-to-voice calls by registering in the national "Do Not Call" register.** ***Justification: It is clearly unreasonable to require individuals to object to being on dozens, if not hundreds, of individual companies' databases.***
5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected.	5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected.
6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications.	6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner **and free of charge**, to receiving further marketing communications. **Any use of masked sender identities, false contact information or false return addresses or numbers for direct marketing purposes shall be prohibited.** *Justification: In line with WP29 opinion. The prohibition on false return addresses exists today in Article 13(4) of the e-Privacy Directive.*
7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.	7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.

Original Text Relevant Recitals – Article 16	EDRi proposed amendments
RECITALS 32-36	**RECITALS 32-36**
(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users **using electronic communications services** . In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by **other** non-profit organisations to support the purposes of the organisation.	(32) In this Regulation, direct marketing refers to any form of advertising **or similar promotion** by which a natural or legal person sends**, direct or presents** direct marketing communications directly to one or more identified or identifiable end-users **over an electronic communications network**. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties **or members of political parties** that contact natural persons via electronic communications services in order to promote their parties**, candidacy in elections or other political campaigns.** The same should apply to messages sent by non-profit organisations to support the purposes of the organisation. *Justification: In line with WP29 opinion. It's important that the definition of direct marketing is up-to-date with today's technological realities where direct marketing messages are presented (targeted) to citizens in a number of ways.*
	(32a) new Communication to elected representatives or public authorities on matters of public policy, legislation or other activities of democratic institutions should not be regarded as direct marketing for the purpose of this Regulation. *Justification: WP29 recommends amendment to ensure that contact to elected officials does not fall under the ban on direct marketing.*
(33) Safeguards should be provided to protect end-users against unsolicited communications for direct marketing purposes, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, emails, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life **as well as** the legitimate interest of legal persons. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent level of protection for	(33) Safeguards should be provided to protect end-users against unsolicited communications for direct marketing purposes, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, emails, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are

all **citizens** throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.	sent, **directed or presented** to end-users **who are natural persons, including natural persons working for legal persons,** in order to effectively protect individuals against the intrusion into their private life**. Member States should also ensure that that** the legitimate interest of legal persons **with regard to unsolicited communications are protected**. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent level of protection for all **individuals** throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the **electronic contact details in accordance with Regulation (EU) 2016/679 and only for a limited time period.** *Justification: In line with WP29 and EDPS opinions.*
(34) When end-users have provided their consent to receiving unsolicited communications for direct marketing purposes, they should still be able to withdraw their consent at any time in an easy manner. To facilitate effective enforcement of Union rules on unsolicited messages for direct marketing, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes. Unsolicited marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person transmitting the communication or on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to oppose to receiving further written and/or oral marketing messages. (35) In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called **or** present a specific code identifying the fact that the call is a marketing call.	(35) In order to allow easy withdrawal of consent,

(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish and or maintain national systems only allowing such calls to end-users who have not objected.	legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to- voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called **and** present a **specific code identifying the fact that the call is a marketing call.** *Justification: WP29 opinion.* (36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish **and or maintain national systems only allowing such calls to end-users who have not objected. End-users should be able to object to future calls from a specific company or organisation during the call from that company or organisation. Member States should also ensure that end-users can object to all future voice-to-voice direct marketing calls by registering their objection in the national "Do Not Call" register.** **A user-friendly option to object to all future calls should be provided free of charge.** *Justification: In line with WP29 opinion. Citizens should not be required to register with every company that may contact them in voice-to-voice marketing calls.*

Original Text	**EDRi proposed amendments**
ARTICLE 17	**ARTICLE 17**
Article 17 Information about detected security risks In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any	Article 17 Information about detected security risks In the case of a particular risk that may compromise the security of **the terminal equipment**, networks and electronic communications services, the provider of an electronic communications service**, the software provider and the terminal equipment vendor** shall inform **all** end-users concerning such risk and, where the risk lies outside

possible remedies, including an indication of the likely costs involved.	the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved. ***Justification: to ensure that the scope of this provisions covers the joint responsibilities of those actors to inform end-users about security risks.***

Original Text	**EDRi proposed amendments**
Relevant Recital – Article 17	
RECITAL 37	
(37) Service providers who offer electronic communications services should inform end- users of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679.	**No amendments proposed**

Original Text	**EDRi proposed amendments**
ARTICLE 18	
CHAPTER IV INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT Article 18 Independent supervisory authorities 1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.	**No amendments proposed**

2. The supervisory authority or authorities referred to in paragraph 1 shall cooperate whenever appropriate with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code].	

Original Text	**EDRi proposed amendments**
ARTICLE 19	
Article 19 European Data Protection Board The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have competence to ensure the consistent application of this Regulation. To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679. The Board shall also have the following tasks: (a) advise the Commission on any proposed amendment of this Regulation; (b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation.	**No amendments proposed**

Original Text	**EDRi proposed amendments**
ARTICLE 20	
Article 20 Cooperation and consistency procedures Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII of Regulation (EU) 2016/679 regarding the matters covered by this Regulation.	**No amendments proposed**

Original Text	EDRi proposed amendments
ARTICLE 21	
CHAPTER V REMEDIES, LIABILITY AND PENALTIES Article 21 Remedies 1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, **and** 79 of Regulation (EU) 2016/679. 2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation and having a legitimate interest in the cessation or prohibition of alleged infringements, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.	CHAPTER V REMEDIES, LIABILITY AND PENALTIES Article 21 Remedies 1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78,–79 of Regulation (EU) 2016/679. 2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation and having a legitimate interest in the cessation or prohibition of alleged infringements, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements. **3. (new) End-users shall have the right to mandate a non-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of protection of their personal data and the protection of privacy to lodge the complaint on his or her behalf, to exercise the rights referred to in paragraphs 1 and 2 of this Article on his or her behalf, and to exercise the right to receive compensation referred to in Article 22 on his or her behalf where provided for by Member State law.** **4. (new) Member States may provide that a body, organisation or association independently of the end-user's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to paragraph 1 of this Article and to exercise the rights referred to in paragraph 2 of this Article if it considers that the rights of the end-user under this Regulation have been**

	infringed. **Justification:** **In order to comply with its main purpose, this Regulation has to "particularise and complement" the GDPR. Now, the GDPR provides several remedies among which, a collective redress mechanism. The provision in the earlier leaked version of the proposed Regulation has to be re-introduced in order to uphold data subjects' rights. Even though Article 21.2 makes a referral to such a mechanism, it does not explain the concept of "legitimate interest" and makes no reference to Article 80 of the GDPR.**

Original Text **Article**	**EDRi proposed amendments**
ARTICLE 22	
Article 22 Right to compensation and liability Any end-user of electronic communications services who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered, unless the infringer proves that it is not in any way responsible for the event giving rise to the damage in accordance with Article 82 of Regulation (EU) 2016/679.	**No amendments proposed**

Original Text **Article**	**EDRi proposed amendments**
ARTICLE 23	
Article 23 General conditions for imposing administrative fines 1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation. 2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1,	**No amendments proposed**

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 Article 8; (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; (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. 4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17. 5. Non-compliance with an order by a supervisory authority as referred to in Article 18, shall 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. 6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. 7. The exercise by the supervisory authority of its powers under this Article shall be subject to	

appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process. 8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.	

Original Text **Article**	**EDRi proposed amendments**
ARTICLE 24	
Article 24 Penalties 1.Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than 18 months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.	**No amendments proposed**

Original Text **Article**	**EDRi proposed amendments**
ARTICLE 25	
	No amendments proposed

CHAPTER VI DELEGATED ACTS AND IMPLEMENTING ACTS Article 25 Exercise of the delegation 1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. 2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation]. 3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. 4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016. 5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. 6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and	

the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	

Original Text	**EDRi proposed amendments**
Article	
ARTICLE 26	
Article 26 Committee 1. The Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code]. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011 12 . 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	**No amendments proposed**

Original Text	**EDRi proposed amendments**
Article	
ARTICLE 27	
CHAPTER VII FINAL PROVISIONS Article 27 Repeal 1. Directive 2002/58/EC is repealed with effect from 25 May 2018. 2. References to the repealed Directive shall be construed as references to this Regulation.	**No amendments proposed**

Original Text	**EDRi proposed amendments**
Article	
ARTICLE 28	

Article 28 Monitoring and evaluation clause By 1 January 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation. No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.	Article 28 Monitoring and evaluation clause **Six months before enter into force of this Regulation** at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation. No later than **two** years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.

Original Text **Article**	**EDRi proposed amendments**
ARTICLE 29	
Article 29 Entry into force and application 1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. 2. It shall apply from 25 May 2018. This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at Brussels, For the European Parliament The President For the Council The President	**No amendments proposed**