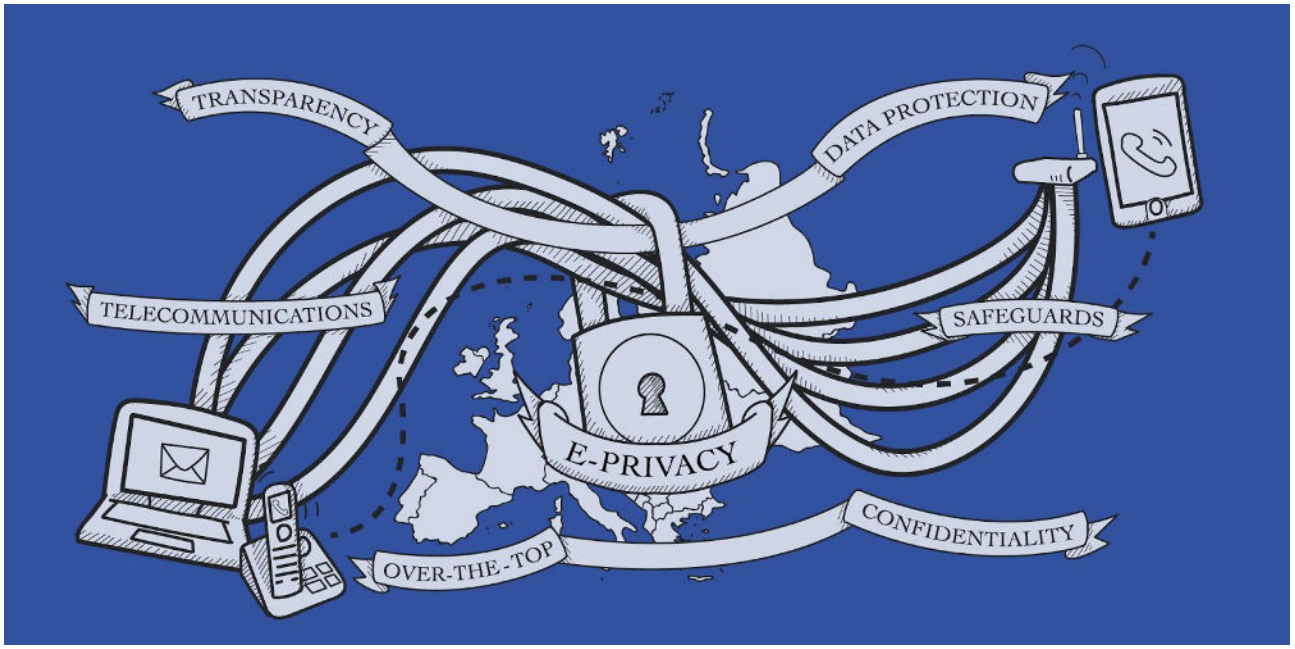
Access Now's comments to the proposed e-Privacy Regulation



On January 2017, the European Commission tabled a proposal for a 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), also known as the ePrivacy Regulation.

Access Now welcomes the proposal which aims at upgrading the rules on the right to privacy and the confidentiality of communications to today's digital era. We have taken an active role in the review of this important legal instrument, by providing comments to the EU Commission consultation of Spring 2016 and policy recommendations in December 2016. Access Now supports the development of an e-Privacy Regulation, a central piece of legislation for the development of a digital single market that would provide users with a high standard of privacy protection, help restore trust in businesses, and promote the use of tools to fight surveillance. On that basis, we have analysed below the Commission's proposal and proposed amendments to improve the future Regulation.

For More Information, Please Contact

Fanny Hidvégi | European Policy Manager | fanny@accessnow.org
Estelle Massé | Senior Policy Analyst | estelle@accessnow.org

Original proposal	Access Now proposed amendments
(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, including when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the ***communicating*** 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.
Access Now comments: The proposed modifications seek to bring clarity to the scope of application of the legislation.	

Original proposal	Access Now proposed amendments
(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc.	(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc. ***The protection of confidentiality of communications is also 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***

	expression and information.
Access Now comments: The proposed amendment further explain the relevance of the legislation.	

Original proposal	**Access Now proposed amendments**
(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, 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***~~ ***specifically concerns*** the definition of consent under Regulation (EU) 2016/679 ***and the rules on data breach.*** When reference is made to consent by an end-user ***using a device or service***, ~~***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.
Access Now comments: This Regulation cannot change the material scope of the GDPR. Therefore, the applicability to legal persons should be limited to certains rights and rules.	

Original proposal	**Access Now proposed amendments**
(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.	(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***~~ ***are generally*** personal data as defined in Regulation (EU) 2016/679~~***.***~~ ***, in the form of spoken words, text messages, files exchanged among others but also related to elements of these communications, such as metadata.***
Access Now comments: The proposed amendment seeks to add clarity.	

Original proposal	Access Now proposed amendments
(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 ***~~does~~ must*** 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 ***networks and*** services should only be permitted in accordance with this Regulation.
Access Now comments: This Regulation, as *lex specialis* complementing and particularising the GDPR, should not lower the level of protection already guaranteed, but rather build additional protection on the general basis established under the GDPR. This amendment does not, however, guarantee that the ePrivacy Regulation meets that standard, but it is important to recall this objective. The last proposed changes in this amendment aims at ensuring consistency with the scope of application of this Regulation to both communications network and services providers.	

Original proposal	Access Now proposed amendments
(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.	(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.
Access Now comments: /	

Original proposal	Access Now proposed amendments
(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	***deleted***

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.	
Access Now comments: We would like to caution over the risk of divergent interpretation or clarification by Member States which can lead to unequal rights for end-users and conflicting rules for the industry. We therefore suggest to delete this recital.	

Original proposal	**Access Now proposed amendments**
(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 ***~~should~~ 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***, processed*** or stored in end-users' terminal equipment.
Access Now comments: This amendment brings legal certainty by clarifying the effect of the Regulation.	

Original proposal	**Access Now proposed amendments**
(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 end-users in the Union.	(9) This Regulation ***~~should~~ sets forth rules that*** 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 end-users in the Union.
Access Now comments: This amendment brings legal certainty by clarifying the effect of the Regulation.	

Original proposal	**Access Now proposed amendments**
(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	(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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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.	(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~~ confidentiality, irrespective of the medium chosen or used***, this Regulation ***~~uses the~~ provides its own*** 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***, such as internal messaging, newsfeeds, closed groups, timelines and similar functions in online services where messages are exchanged with other users within or outside that service***; therefore, such type of services also having a communication functionality should be covered by this Regulation.
Access Now comments: To ensure legal certainty and dependance on definitions to be set in a instrument that is currently being negotiated, the Regulation should include its own set of definition, as recommended by the opinion of the Article 29 Working Party on Data Protection.	

Original proposal	Access Now proposed amendments
(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.	(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.
Access Now comments: /	

Original proposal	Access Now proposed amendments
(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.	(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' ***and*** situated at different places within a city, ***such as*** department stores, shopping malls and hospitals ***etc***, ***as well as Wi-Fi access offered to visitors and guests at airports, hotels, restaurants. These hotspots and Wi-Fi might require to login or provide a password and may be provided by public administrations.*** 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 ***an organisation*** ~~***the corporation***~~.
Access Now comments: This amendment brings clarity to the applicability of the law and ensure that end-users rights will be widely protected, as recommended in the European Data Protection Supervisor's opinion.	

Original proposal	**Access Now proposed amendments**
(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 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. ***The exclusion of services providing "content transmitted using electronic communications networks" from the definition of "electronic communications service" in Article 4 of this Regulation does not mean that service providers who offer both electronic communications services and content services are outside the scope of the provisions of the Regulation which applies***

	to the providers of electronic communications services. 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.
Access Now comments: This amendment brings clarity to what constitutes metadata and bring legal certainty by ensuring that these data will be protected under the Regulation. It also includes clarification suggested by the Article 29 Working Party in their opinion.	

Original proposal	**Access Now proposed amendments**
(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.	(15) Electronic communications data sh***all~~ould~~*** be treated as confidential. This means that 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, ***~~without the consent of all the communicating parties~~ by persons other than the end-users*** should be prohibited. The prohibition of interception of communications data should ***also*** apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee***, and when stored***. 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. ***To protect their fundamental right to privacy, natural persons shall have the right to object pursuant to Article 19 of the Regulation (EU)***

	2016/679, to the creation of profile about him or her. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, ***and analysis of customers' traffic data,*** including browsing habits without the end-users' consent.
Access Now comments: This amendment brings consistency with Article 5 and brings necessary additional protection for natural persons.	

Original proposal	**Access Now proposed amendments**
	(15 a - new) For the purpose of provision in Article 6 paragraph 1 point (a) of this Regulation, "transmission" means "the processing of communication data to and from the end-user and includes all technologies and services of the provider that are required and used only to accomplish this specific purpose".
Access Now comments: This amendment is based on suggestion from the European Disability Forum to ensure that accessibility services will be fully functioning. The language covers the bi-directional nature of communication and the fact that providers can use whatever technologies and services are required to get the communication to the end-user as long as those technologies and services are only used for that purpose only. This particular language does not require the service or network providers to provide any extraordinary technologies or services but allows such technologies and services to be provided if it is necessary for the purpose of transmitting a communication.	

Original proposal	**Access Now proposed amendments**
(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.	(16) The prohibition of storage of ***metadata*** ~~***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.
Access Now comments: This amendment limits the possibility for companies to store content data as it would constitute a disproportionate interference with people's rights to privacy and data protection.	

Original proposal	**Access Now proposed amendments**

(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 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.	(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 time, an identifier ***may be*** ~~***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***~~. When***re 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.
Access Now comments: The changes proposed in this amendment increase users' protection, bring consistency, by ensuring that all metadata are protected and that their used is carefully monitored and overseen.	

Original proposal	**Access Now proposed amendments**
(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) ***Processing of metadata, by providers of electronic communications services, may be permitted in certain limited circumstances, for specified and clearly defined purposes and under clearly defined conditions.*** 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. ***Such services usually exposes end-users to serious privacy and data protection risks which should be clearly communicated to the end-users.*** 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. ***End-users should receive all relevant information about the intended processing in a clear and easily understandable language, such information should be given separately from the terms and conditions to the services.***
Access Now comments: The amendment brings clarity to the use of metadata and aims at providing greater information to end-users.	

Original proposal	**Access Now proposed amendments**
(19) The content of electronic communications pertains to the essence of the fundamental	(19) The content of electronic communications pertains to the essence of the fundamental

right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.	right to respect for private and family life, home and communications protected under Article 7 of the Charter. ~~***Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse.***~~ This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of ~~***all***~~ the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material***, such as spam, if the content is accessible***. ***Providers of electronic communications services shall not try to or be forced to comply with a request to gain access to content that is protected by technical means.*** 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.***~~
Access Now comments: This amendment provides clarity from a legal and technical perspective to ensure that providers of electronic communications services only gain access to what is strictly necessary for a specific purpose and that end-users' rights to privacy and confidentiality of communications remain protected.	

Original proposal	**Access Now proposed amendments**

(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 ***processed by or*** 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 ***often*** without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information ***processed by or*** 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 ***explicit*** consent and for specific***, limited,*** and transparent purposes. ***End-users should receive all relevant information about the intended processing in a clear and easily understandable language, such information should be given separately from the terms and conditions to the services.***
Access Now comments: The proposed changed bring legal certainty and and aims at providing	

greater information to end-users.

Original proposal	**Access Now proposed amendments**
(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. 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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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	(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 ***prevent the use of so-called "cookie-walls" and "cookie-banners" that have not helped users maintain control over their personal information and privacy or become informed about their rights. This Regulation should***

enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.	provide for the possibility to express consent by ***technical specifications by for instance*** using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.
Access Now comments: This amendment brings clarity on the need to ban so-called "cookie-wall" and "cookie-banner".	

Original proposal	**Access Now proposed amendments**
(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***~~ ***by default*** prevent***s cross-domain tracking and*** third parties from storing information on the terminal equipment; this is often presented as 'reject third party ***trackers and*** cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept ***trackers and*** cookies') to lower (for example, 'always accept ***trackers and*** cookies') and intermediate (for example, 'reject ~~***third party***~~ ***all trackers and*** cookies ***that are not strictly necessary in order to provide a service explicitly requested by the user'*** or ***'reject all cross-domain tracking'*** ~~***'only accept first party cookies'***~~). Such privacy

	settings should be presented in ~~a~~ an easily visible***, objective*** and intelligible manner. ***For web browsers, applications, products and 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 signify his or her freely given, specific, informed, and explicit agreement to the storage and access of such cookies or 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. 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 trackers 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 or sharing with more third parties. Web browsers, applications, products and services 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 trackers and cookies are always or never allowed. In case of no active choice, or action from the user, the web browsers shall be set by default that it rejects and blocks the storage of trackers, including cookies, that are not strictly necessary in order to provide an information society service explicitly requested by the user.***
Access Now comments: This amendment joints recital 23 and 24 into a single place for clarity and modify language on trackers to ensure that users' confidentiality and privacy are protected no matter the technology used.	

Original proposal	**Access Now proposed amendments**
(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	***deleted***

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.	
Access Now comments: The content of this recital was moved to recital 23.	

Original proposal	**Access Now proposed amendments**
(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	(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer

tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages 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.	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. ***Currently***, this information ***~~may be~~ 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. ***~~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.~~ Therefore, only in a limited number of circumstances and only if the used data would be anonymised and deleted after the strictly defined and limited in time collection purpose 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 o her consent.*** Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.
Access Now comments: This amendment aims at bringing clarity and reflect improvements suggested by Article 29 Working Party.	

Original proposal	**Access Now proposed amendments**
(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	(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation ***~~should provide for~~ is without prejudice to*** the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights ***set***

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).	***under this Regulation*** when such a restriction ***is targeted to suspects, requires prior judicial authorisation or by an independent authority, and*** 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. ***Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.*** 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).
Access Now comments: The modification suggested in this amendment would bring the text in line with the jurisprudence of the Court of Justice of the European Union in joint cases C-293/12 and C-594/12.	

Original proposal	**Access Now proposed amendments**
(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	(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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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.	(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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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.	(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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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	(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.	(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.~~***
Access Now comments: The amendment ensures that users will not be unduly prevented from the ability to contact entities and request information that might be necessary to exercise their right to remedy.	

Original proposal	**Access Now proposed amendments**
(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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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	(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.	non-profit organisations to support the purposes of the organisation.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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 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.	(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 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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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	(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

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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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, 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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(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.	(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 ***given their consent*** ~~***not objected***~~.
Access Now comments: A positive and active action from end-users should be required to ensure that they have been informed and are exercising their rights.	

Original proposal	**Access Now proposed amendments**
(37) Service providers who offer electronic	(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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(38) To ensure full consistency with Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.	(38) To ensure full consistency with Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement	(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement

of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.	of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(40) In order to strengthen the enforcement of the rules of this Regulation, each supervisory authority should have the power to impose penalties including administrative fines for any infringement of this Regulation, in addition to, or instead of any other appropriate measures pursuant to this Regulation. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. For the purpose of setting a fine under this Regulation, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 of the Treaty.	(40) In order to strengthen the enforcement of the rules of this Regulation, each supervisory authority should have the power to impose penalties including administrative fines for any infringement of this Regulation, in addition to, or instead of any other appropriate measures pursuant to this Regulation. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. For the purpose of setting a fine under this Regulation, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 of the Treaty.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the	(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the

Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016 8 . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.	Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016 8 . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
(42) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural and legal persons and the free flow of electronic communications data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what	(42) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural and legal persons and the free flow of electronic communications data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond

is necessary in order to achieve that objective. (43) Directive 2002/58/EC should be repealed.	what is necessary in order to achieve that objective. (43) Directive 2002/58/EC ***and Commission Regulation (EU) 611/2013*** should be repealed.
Access Now comments: The Regulation setting forth specific rules on data breach notification should be repealed as the Regulation (EU) 2016/679 will apply and its legal basis, Directive 2002/58/EC will be repealed.	

Original proposal	**Access Now proposed amendments**
CHAPTER I **GENERAL PROVISIONS** *Article 1* *Subject matter*	**CHAPTER I** **GENERAL PROVISIONS** *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. 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. 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.	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. 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.
Access Now comments: */*	

Original proposal	**Access Now proposed amendments**
Article 2 *Material Scope*	*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	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 ***or processed by*** the

end-users.	terminal equipment of end-users.
Access Now comments: This amendment brings clarity to the scope of the information that should be protected.	

Original proposal	**Access Now proposed amendments**
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;	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;
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
Article 3 *Territorial scope and representative* 1. This Regulation applies to:	*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 terminal equipment of end-users located in the Union.	(a) the provision of electronic communications services to end-users ***who are*** in the Union, ***regardless of whether the provider of services is from inside Union or not, regardless of whether the processing of the communications services takes place in the Union or not and*** irrespective of whether a payment of the end-user is required; (b) the use of such services; (c) the protection of information related to ***or processed by*** the terminal equipment of end-users ***who are ~~located~~*** in the Union. ***(d) the provision of electronic communications services from outside the Union, but in a place where Member State law applies by virtue of public international law.***
Access Now comments: This amendment clarifies the territorial scope of the law to ensure that all end-users protected under the Charter will be protected under the Regulation.	

Original proposal	**Access Now proposed amendments**
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. 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. 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.	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. 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, ***courts*** and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation. 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.

	6. The representative can be the same as the one designated under Article 27 of Regulation (EU) 2016/679.
Access Now comments: This amendment seeks to clarify the power of the designated representative.	

Original proposal	**Access Now proposed amendments**
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]; (c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC 10.	*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' ***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;*** ,***~~'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];~~*** (c) ***'electronic communications service' means a service, provided for remuneration or not, 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; ***(d) 'interpersonal communications service' means a service, provided for remuneration or not, that enables direct interpersonal and interactive exchange of information via all electronic communications networks. This includes services which enable interpersonal communication merely as an 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 parlty or fully as its addressing system;*** ***(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' means a natural person using or requesting a publicly available electronic communications service;*** ***(h) 'end-user' means a user not providing public communications networks or publicly available electronic communications services;*** ***(i)*** the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC 10***;*** ***(j) web audience measuring means the counting of connections on a specific***

	website, webpage, or service for the purpose of measuring results and calculate traffic without identifying, attributing an identifier or trackings any of these connections.
Access Now comments: To ensure legal certainty and avoid dependence on definitions to be set in an instrument that is currently being negotiated, the Regulation should include its own set of definitions, as recommended by the opinion of the Article 29 Working Party on Data Protection. Certain definitions have als been slightly modified to better fit the scope of the ePrivacy Regulation and ensure that the provisions are technologically neutral.	

Original proposal	**Access Now proposed amendments**
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: (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; (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; (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;	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: (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 ***or via electronic communications networks***, such as text, voice, videos, images, and sound; (c) 'electronic communications metadata' means data processed ***~~in an electronic communications network~~*** for the purposes of transmitting, distributing or exchanging electronic communications content; including ***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 about, broadcasted or emitted, and stored 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.***

(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.; (g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems; (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.	(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; (f) ‘direct marketing communications’ means any form of advertising, whether written or oral, sent***, directed or presented*** 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, ***targeted advertising on online webpages,*** electronic mail, SMS, etc.; (g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems; (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.
Access Now comments: The suggested amendment suggest the deletion of point 2 as it was moved to point 1. The further proposed edits aims at providing clarity on what constitutes metadata to ensure a robust and harmonised level of protection.	

Original proposal	**Access Now proposed amendments**
CHAPTER II **PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT**	**CHAPTER II** PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION ***~~STORED IN~~ PROCESSED BY AND RELATED***

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.	***TO*** 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.
Access Now comments: The amendment clarifies the scope of application of this chapter and or Article 5 to prevent loopholes in the protection of confidentiality of communications.	

Original proposal	**Access Now proposed amendments**
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. 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 for the duration necessary for that purpose; or (b) it is necessary for billing, calculating	*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 ***strictly*** necessary to achieve the transmission of the communication, for the duration necessary for that purpose ***only***; or ***(aa) it is strictly necessary for providing an information society service explicitly requested by the end-user, provided that the provision of that service cannot be fulfilled without the processing of such data. Such processing of personal data must be conducted pursuant Regulation (EU) 2016/679, in particular Articles 5 and 12; 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***. ***(c) Providers of electronic communications networks and services shall not try to or be forced to comply with a request to gain***

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.	***access to end-users' content that is protected by technical means, including when complying with point (a) and (b).*** 2. Providers of electronic communications services may process electronic communications metadata ***only*** 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 for the duration necessary for that purpose; or (b) it is ***strictly*** necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or ~~***abusive***~~ ***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 ***requested by that*** ~~***to such***~~ end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous. ***(d) Where a processing of electronic communications metadata is taking place, Articles 35 and 36 of Regulation (EU) 2016/679 shall apply.***
Access Now comments: The proposed amendment seeks to enhance users' rights to privacy and confidentiality, by limiting the use of content data and metadata by providers to what is strictly necessary for identified and clearly defined purposes, in line with principles defined in Regulation (EU) 2016/679. Point 1 (aa) was added to ensure the functioning of accessibility services requested by users with a disability.	

Original proposal	**Access Now proposed amendments**
3. Providers of the electronic communications services may process electronic communications content only: (a) for the sole purpose of the provision of a	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 consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.	specific service ~~***to***~~ ***requested by that*** ~~***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***~~ ***In such cases,*** the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.
Access Now comments: The proposed amendment seeks to enhance users' rights to privacy and confidentiality, by limiting the use of content data to what is strictly necessary, due to the intrusiveness of this practice.	

Original proposal	**Access Now proposed amendments**
Article 7 *Storage and erasure of electronic communications data* 1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679. 2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication. 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 relevant metadata may be kept	*Article 7* *Storage and erasure of electronic communications data* 1. Without prejudice to point (b) of Article 6(1) and points (a) and ***(aa)*** ~~***(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 metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the ~~***relevant***~~ ***necessary*** metadata

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.	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.
Access Now comments: Based on experience from the implementation of the Directive 2002/58/EC, the use of anonymised data have led to abuse of end-users rights by providers of services and should therefore be prevented. For more information, please see Access Now's position paper on the ePrivacy Regulation: https://www.accessnow.org/cms/assets/uploads/2016/12/Access-Now-ePrivacy-Directive-policy-paper.pdf	

Original proposal	**Access Now proposed amendments**
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 (c) it is necessary for providing an information society service requested by the end-user; or (d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user. 2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if: (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or (b) a clear and prominent notice is displayed informing of, at least, the modalities of the	*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~~ processing*** of information from end-users' terminal equipment, including ***information*** about its software and hardware ***and any electronic communications data***, 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 ***concerned*** end-user has given his or her consent; or (c) it is ***strictly*** necessary for providing an information society service ***explicitly*** requested by the end-user***~~; or~~*** (d) if it is ***strictly*** necessary for web audience measuring ***as defined under this Regulation***, provided that such measurement is carried out by the provider of the information society service requested by the end-user ***and that tracking is not taking place as a result of this practice***. ***(e) No end-user shall be denied access to any communications services, regardless of whether these services are remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to***

collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection. The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied. 3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner. 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.	***the processing of personal information and/or the use of storage capabilities of his or her terminal equipment(s) that is not necessary for the provisions of those services.*** ***(f) No end-users shall be denied any functionality of a connected device or product, regardless of whether the use of a device is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) for processing information and/or the use of storage capabilities of his or her terminal equipment(s) that is not necessary for the functionality requested.*** 2. The ~~***collection***~~ ***processing*** of information emitted by terminal equipment ~~***to enable it to connect to another device and, or to network equipment***~~ shall be prohibited, except if: (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection***, which the end-users have requested and authorised****;* or (b) ***the end-user has given his or her consent to the processing of his or her location data for a specific purpose, including for the provision of specific services to the concerned end-users, provided that the defined purpose could not be fulfilled without processing this information.*** ~~***a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection. The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.***~~ ~~***3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in***~~

	~~order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.~~ ***~~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.~~***
Access Now comments: This amendments reflects the clarification suggested by the opinions of the Article 29 Working Party and the EDPS to close significant loopholes for the protection of end-users' rights.	

Original proposal	**Access Now proposed amendments**
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. 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.	*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 ***as set forth under Regulation (EU) 2016/679*** may be expressed by using ***technical specifications of electronic communications services*** ***~~the appropriate technical settings of a software application enabling access to the internet.~~*** 3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2)***, ~~and~~*** point***~~s~~*** (a) ***~~and (b)~~*** of Article 6(3) ***and point (b) of Article 8(1)*** 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.
Access Now comments: The following amendment aims at ensuring that legislation remains technologically neutral and does not limit the possibility for end-users to express consent via web browser.	

Original proposal	**Access Now proposed amendments**
Article 10 *Information and options for privacy settings to be provided*	*Article 10* ***~~Information and options for pP~~****rivacy* ***by design and by default ~~settings to be~~***

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. 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. 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.	~~***provided***~~ 1. ***The settings of all the components of the terminal equipment shall be configured to, by default, prevent third parties from storing information, processing information already stored in the terminal equipment and preventing the use of the equipment's processing capabilities by third parties.*** 2**.** Software ***and operating systems*** ~~***placed on the market***~~ permitting electronic communications, including the retrieval and presentation of information on the internet, shall ***be configured by default*** ~~***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***, and prevent the use of others trackers***. ***3***. Upon installation, the software ***and operating systems*** 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. 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.
Access Now comments: The amendment brings the text in line with the principles of privacy by design and by default, which are central to the protection of privacy and confidentiality of communications and ensures that hardwares, and not only softwares, placed on the market will be protected. This amendment introduces measures that will increase products and services security and therefore bring trust in the market, as well as benefiting users' rights.	

Original proposal	**Access Now proposed amendments**
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) of	*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 suspects of serious crime, and*** respects the ~~***essence of the***~~ fundamental rights and freedoms and is a necessary, appropriate and proportionate measure, ***including prior judicial authorisation or by an independent***

Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. 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.	***authority***, in a democratic society to safeguard ***defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication systems.*** ~~***one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests***~~. ***Any legislative measure referred to in this paragraph shall be in accordance with the Charter of Fundamental Rights of the European Union.*** 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. ***Providers of electronic communications services shall keep details about requests made pursuant to paragraph 1, which shall be made available to the competent supervisory authority upon request. This shall include:*** ***(a) the in-house staff member who handled the request;*** ***(b) the identity of the official or body asking for the information;*** ***(c) the purpose for which the information was sought;*** ***(d) the date and time of the request;*** ***(e) the legal 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;*** ***(f) the number of end-users to whose data the request related;*** ***(g) the data provided to the requesting official or body;*** ***(h) the period covered by the data.*** ***3. All providers of electronic communications services shall provide every year to the competent supervisory***

	authority and to the public, a transparency report, providing the number of requests received pursuant to paragraph 1, from which authorities, the number of granted requests, and the numbers of end-users affected by the requests. Such transparency reporting shall also include information about privacy and data protection practices and policies, inform users about avenues for remedies in case of abuses and feature clear and easily understandable information about end-users rights protected under this Regulation. ***4. Providers of electronic communications services shall be subject to enforcement actions by the competent authority including fines pursuant to paragraph 2 of Article 23 of this Regulation.***
Access Now comments: This amendment seeks to bring the text in line with the jurisprudence of the CJEU. It is important to note that the exception foreseen under paragraph 1 should only be allowed in the context of serious crimes, even if the definition of what constitute a serious crime is still being developed and would require greater legal certainty. The amendment also introduces a mandatory obligation for provider of electronic communications services to produce a yearly and publicly available transparency report.	

Original proposal	**Access Now proposed amendments**
CHAPTER III **NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS** *Article 12* *Presentation and restriction of calling and connected line identification*	**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:	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;	(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;
(b) the called end-user with the possibility of	(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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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	*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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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.	*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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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 directory 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 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. 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	*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 directory 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 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. 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. 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.	obtain end-users' consent before enabling such search functions related to their own 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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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. 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. 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.	*Article 16* *Unsolicited communications* 1. Natural or legal persons may ***only*** use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons ***if he or she ~~that~~*** ha***~~ve~~*** given their consent. 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. 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 expressed their objection to receiving those communications. 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. 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.	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 expressed their objection to receiving those communications. 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, ***object to the processing of their information and regarding the lodging of a complaint,*** in an easy manner, to receiving further marketing communications. 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.
Access Now comments: The amendment aims at strengthening end-users' rights.	

Original proposal	**Access Now proposed amendments**

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 possible remedies, including an indication of the likely costs involved.	*Article 17* *Information about detected **and known** security risks* ***1.*** In the case of a particular risk that may compromise the security of ***the terminal equipment,*** networks ***or ~~and~~*** electronic communications services, the ***relevant*** provider of an electronic communications service**, network provider and/or terminal equipment provider** shall inform ***all*** 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 possible remedies, including an indication of the likely costs involved. ***2. In case of data breach, Article 33 and 34 of Regulation (EU) 2016/679 shall apply.***
Access Now comments: The amendment clarifies the obligation of all actors in the market as well as protecting end-users.	

Original proposal	**Access Now proposed amendments**
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. 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].	**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. 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].
Access Now comments: /	

Original proposal	**Access Now proposed amendments**

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.	*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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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.	*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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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,	**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.	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. ***3. An end-user or a group of 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. A body, organisation or association independently of the end-user's mandate, shall have the right to lodge, in the Member State where it is registered, 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.***
Access Now comments: In order to complement and particularise Regulation (EU) 2016/679, this amendment provides for a right of representation for end-users and a right to collective redress to increase avenues for remedy and assist competent supervisory authority in the implementation of this Regulation and in the protection of end-users' rights.	

Original proposal	**Access Now proposed amendments**
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	*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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
Article 23 *General conditions for imposing administrative fines*	*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.	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, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:	2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;	***~~(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;	***~~(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;~~***
(c) the obligations of the providers of publicly available directories pursuant to Article 15;	(c) the obligations of the providers of publicly available directories pursuant to Article 15;
(d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.	(d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.
3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.	***(e) The obligation to publish an annual transparency report set out by Article 11.*** 3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5 ***to 10 ~~, 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
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.	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.
Access Now comments: The proposed amendment would bring consistency to the addition brought to Article 11.	

Original proposal	**Access Now 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.	*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.
Access Now comments:	

Original proposal	**Access Now proposed amendments**
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	**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

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.	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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	*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. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
CHAPTER VII **FINAL PROVISIONS** *Article 27* *Repeal* 1. Directive 2002/58/EC is repealed with effect from 25 May 2018.	**CHAPTER VII** **FINAL PROVISIONS** *Article 27* *Repeal* 1. Directive 2002/58/EC ***and Commission Regulation 611/2013 are ~~is~~*** repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation.	2. References to the repealed Directive shall be construed as references to this Regulation.
Access Now comments: This amendment brings consistency and ensure that two separate framework on data breach will apply as the rules set forth under Regulation (EU) 2016/679 will apply and its legal basis, Directive 2002/58/EC will be repealed.	

Original proposal	**Access Now proposed amendments**
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* 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.
Access Now comments: /	

Original proposal	**Access Now proposed amendments**
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.	*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.
Access Now comments: /	