European Parliament
2014-2019

Committee on Legal Affairs

2017/0003(COD)

5.10.2017

OPINION

of the Committee on Legal Affairs

for the Committee on Civil Liberties, Justice and Home Affairs

on the 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)
(COM(2017)0010 – C8-0009/2017 – 2017/0003(COD))

Rapporteur: Pavel Svoboda

PA_Legam

SHORT JUSTIFICATION

The rapporteur does **not** welcome the proposal concerning the respect for private life and the protection of personal data in electronic communications ('ePrivacy Regulation').

All the aims of the creation of a digital single market (growth, promoting innovation, boosting Europe's IT-based economy, the free flow of data, and promotion of SMEs) will not be attained, and in some cases indeed the very opposite of what is intended will be brought about. Many existing business models would be outlawed by this.

The proposal would generate serious legal inconsistency with Regulation (EU) No 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - 'GDPR') and with the proposal concerning the European Electronic Communications Code ('EECC') and bring about extreme legal uncertainty regarding the use of data, while having illogical consequences with regard to personal data.

A lack of courage and creativity, and an insistence on clinging to old structures and convictions, are not a good starting point for building a successful digital future.

The proposal should:

1) mainly be concerned with the confidentiality of communication;
2) ensure fair competition in the field of communication and (b) align itself with a global situation;
3) not be a 'lex specialis' concerning the GDPR, but supplement it;
4) avoid duplication of structures provided for by the GDPR (e.g. consent, communication of personal data to third countries, penalties, EDPB, etc.). Personal data should be governed by a single legal framework. Communications data as personal data should on no account be treated separately. The same data ought to be subject to the same law/principles. Article 6 of the GDPR should be amended accordingly;
5) look to the future and accord with the EECC;
6) refrain from focusing on consent. Nowadays, consent is no longer the right criterion; transparency, data sovereignty, opt-out solutions, rights of objection, a new category of data (e.g. pseudonymised data) or at least better differentiation between anonymised, pseudonymised and encrypted data would be a better approach. Moreover, there is a danger that the balance that the GDPR has established between protecting privacy and new technologies may be destroyed again because in large areas data processing which would be permitted under the GDPR would either be subject to even stricter consent conditions or else be entirely prohibited. That is absolutely counter-productive.

Welcome features of the proposal are that:

- the ePrivacy Regulation is brought into line with technical reality and Articles 7 and 8 of the EU Charter of Fundamental Rights;
- the Commission has included provisions concerning Over-the-Top communication services within its scope;
- the Commission wishes to synchronise the time of entry into force with the GDPR. In fact, this will not be practical for businesses to comply with, particularly if the complicated duplication of structures were to be retained.

Specifically:

- Article 4, in particular, is based on the EECC. The ePrivacy Regulation therefore cannot be applied before the EECC has been adopted. This is a systematic error, which must be corrected;
- the proposal does not distinguish clearly between content, data and information;
- The demarcation line between the e-Privacy Regulation and the GDPR is unclear. In the interests of legal certainty, it should be established when one of them applies and when the other does, in order to create a comprehensible legal framework for those responsible. Therefore only personal data should be subject to ePrivacy during the communication process, as stipulated by Directive 2002/58/EC. In all other cases, the GDPR would then apply. The law should also make it clear when a communication ends;
- there must be a clear demarcation line between the confidentiality of the substance of communications and the processing of data (data protection), as the scope of ePrivacy extends to networked devices and machines. Not all of the definitions or of the scope of the proposal are clear. It would consequently have an unpredictable and illogical impact on machine-to-machine communication (e.g. in the car industry, logistics or smart homes). It is not clear where the conveyance of communications under ePrivacy begins and where data transmission under the GDPR begins. It is also unclear what consent, or denial of consent, for machine-to-machine communication would mean;
- the proposal requires consent even for the processing of anonymous data, which is totally illogical and technically impossible. The concept of pseudonymisation, which is implied in the GDPR, could have been built upon here;
- it is also logically unclear why metadata (ePrivacy) in effect have to be better protected than health data (GDPR);
- it is also incomprehensible why two systems of penalties should be introduced for the same offence;
- consideration should be given to whether a household exemption is needed;
- the proposed rule on cookies would favour big businesses and place SMEs (especially those in Europe) at a disadvantage. Precisely the opposite is desirable;
- As currently worded, Article 5 of the proposal could endanger the continued existence of email.

Improvements are needed on many points. The Committee on Legal Affairs therefore calls on the committee responsible to take into account the following amendments:

AMENDMENTS

The Committee on Legal Affairs calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a regulation
Recital 1

Text proposed by the Commission	*Amendment*
(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 ***communications***, including ***information regarding*** when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the ***communication*** parties. The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, ***in-platform messages between users of a social network,*** e-mail, internet phone calls and personal messaging provided through social media.

Amendment 2

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(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. Metadata derived from electronic communications	(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. 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.	may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc. ***The protection of confidentiality of communications is an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, freedom of assembly, freedom of expression and information.***

Amendment 3

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore ***does*** not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data ***by providers of electronic communications services*** should only be permitted in accordance with this Regulation.	(5) The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore ***can*** not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data should only be permitted in accordance with ***and on legal ground specifically provided under*** this Regulation.

Amendment 4

Proposal for a regulation
Recital 6

Text proposed by the Commission	*Amendment*
(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[22] 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[22] 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 ***using the new media***. Those developments include the entrance on the market of electronic communications services ***(including new web-based interpersonal communications services, including online telephone, instant messaging and Internet e-mail)*** 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.
[22] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).	[22] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

Amendment 5

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(7) The Member States should be allowed, within the limits of this	***deleted***

Regulation, to maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. Therefore, the margin of discretion, which Member States have in this regard, should maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.

Amendment 6

Proposal for a regulation
Recital 9

Text proposed by the Commission	*Amendment*
(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 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. ***This should be the case irrespective of whether the electronic communications are connected to a payment or not.***

Amendment 7

Proposal for a regulation
Recital 11

Text proposed by the Commission	*Amendment*
(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users	(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[24]]. 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.	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[24]]. 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, timelines and similar functions in online services where messages are exchanged with other users within or outside that service (i.e. public and privately available newsfeeds and timelines)***; therefore, such type of services also having a communication functionality should be covered by this Regulation.
[24] Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).	[24] Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

Amendment 8

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(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' situated at different places within a city, department stores, shopping malls***, airports, hotels, hostels ,hospitals*** and ***other similar Internet access points***. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be ***adequately*** 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.

Amendment 9

Proposal for a regulation
Recital 14

Text proposed by the Commission	*Amendment*
(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	(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.	processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. ***It should also include location data, such as for example the actual or inferred location of the terminal equipment, the location of the terminal equipment from or to which a phone call or an internet connection has been made, or the Wi-Fi hotspot that a device is connected to, as well as data necessary to identify the terminal equipment of end-users.*** 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.

Amendment 10

Proposal for a regulation
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) Equipment location data should include data transmitted or stored in terminal equipment generated by accelerometers, barometers, compasses, satellite positioning systems or similar sensors or devices.

Amendment 11

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(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 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 ***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. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, ***injecting ads or other content and analysis of customers´ traffic data,*** including browsing habits without the end-

users' consent.

Amendment 12

Proposal for a regulation
Recital 16

Text proposed by the Commission	*Amendment*
(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 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. ***Where a type of processing of electronic communications data for these purposes is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.***

Amendment 13

Proposal for a regulation
Recital 17

Text proposed by the Commission	*Amendment*
(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	(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 colours 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***

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 colours to indicate the presence of individuals. ***This should be done in accordance with Article 25 of Regulation (EU) 2016/679.*** To display the traffic movements in certain directions during a certain period of time, an identifier ***may be*** necessary to link the positions of individuals at certain time intervals. ***When processing*** electronic communications metadata, 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.

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.

Amendment 14

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(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	(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 ***or to instigate certain technical operations or tasks, often without the knowledge of 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**.**

user. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. ***A high and equal level of protection of the private sphere of users' needs to be ensured in relation to the privacy and confidentiality of users' terminal equipment content, functioning and use.*** Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific***, limited,*** and transparent purposes

Amendment 15

Proposal for a regulation
Recital 21

Text proposed by the Commission	*Amendment*
(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	(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***.	online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website ***by the person or legal person in charge*** of the ***website ("first party analytics")***.

Amendment 16

Proposal for a regulation
Recital 21 a (new)

Text proposed by the Commission	*Amendment*
	(21a) Equipment location data can give a very detailed and intrusive insight into an individual's personal life or an organisation's business and activities. Processing of location data from any source, whether electronic communications metadata or equipment location data should be conducted on the basis of clear rules.

Amendment 17

Proposal for a regulation
Recital 22

Text proposed by the Commission	*Amendment*
(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	(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide

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

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 do not help users to maintain control over their personal information and privacy or become informed about their rights. This Regulation should*** provide for the possibility to express consent by ***technical specifications, for instance by*** using the appropriate settings of a browser or other application. ***Those settings should include choices concerning*** the ***storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties. The*** choices made by ***users*** when establishing ***the*** 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 ***user*** to control the flow of information to and from the terminal equipment. More particularly***,*** web browsers***, applications or mobile operating systems*** may be used as ***the executor of the choices of an end-user***, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

Amendment 18

Proposal for a regulation

Recital 23

Text proposed by the Commission	*Amendment*
(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 an easily visible and intelligible manner.	(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent ***by default the cross-domain tracking and*** storing ***of*** information on the terminal equipment ***by other parties***; this is often presented as ′reject third party ***trackers and*** cookies′. End-users should be offered***, by default,*** a set of privacy setting options, ranging from higher (for example, ′never accept ***tracker and*** cookies′) to lower (for example, ′always accept ***trackers and*** cookies′) and intermediate (for example, ′reject ***all trackers and*** cookies ***that are not strictly necessary to provide a service explicitly requested by the user' or 'reject all cross-domain tracking***′). ***These options may also be more fine-grained. Privacy settings should also include options to allow the user to decide for example, whether Flash, JavaScript or similar software can be executed, if a website can collect geo-location data from the user, or if it can access specific hardware*** such ***as a webcam or microphone. Such*** privacy settings should be presented in an easily visible***, objective*** and intelligible manner.

Amendment 19

Proposal for a regulation
Recital 24

Text proposed by the Commission	*Amendment*
(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.	***deleted***

Amendment 20

Proposal for a regulation
Recital 25

Text proposed by the Commission	*Amendment*
(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 personalised 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	(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 personalised 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.	Regulation (EU) 2016/679. ***In addition, such providers should either obtain the end-user's consent or anonymise the data immediately while limiting the purpose to mere statistical counting within a limited time and space and offering effective opt-out possibilities.***

Amendment 21

Proposal for a regulation
Recital 26

Text proposed by the Commission	*Amendment*
(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the	(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security ***(i.e.: state 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

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).	and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. ***Encryption and other security measures are critical to ensure the confidentiality and integrity of electronic communications and the security and integrity of the electronic communications infrastructure as a whole. The measures taken by Member States should not entail any obligations for the provider of the electronic communications network or service that would result in the weakening of the security and encryption of their networks and services.*** Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).

Amendment 22

Proposal for a regulation
Recital 32 a (new)

Text proposed by the Commission	*Amendment*
	(32a) Communication to elected representatives or public authorities on matters of public policy, legislation or other activities of democratic institutions should not be regarded as direct marketing for the purpose of this Regulation.

Amendment 23

Proposal for a regulation
Recital 33

Text proposed by the Commission	*Amendment*
(33) Safeguards should be provided to	(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.	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 ***and only for a limited time period***.

Amendment 24

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(35) In order to allow easy withdrawal of consent, legal or natural persons	(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.

conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called ***and*** present a specific code identifying the fact that the call is a marketing call.

Amendment 25

Proposal for a regulation
Recital 37

Text proposed by the Commission	*Amendment*
(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.	(37) Service providers who offer electronic communications services should ***process electronic*** communications ***data in such a way as to prevent unauthorised access, disclosure or alteration, ensure that such unauthorised access, disclosure or alteration is capable of being ascertained, and also ensure that such electronic communications data are protected*** by using specific types of software ***and*** 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. ***The obligations of Article 40 of the [European Electronic Communications Code] should apply to all services within the scope of this Regulation as regards the security of networks and services and***

related security obligations thereto.

Amendment 26

Proposal for a regulation
Recital 40

Text proposed by the Commission	*Amendment*
(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. ***It should not be permitted to impose double penalties resulting from the violation of both Regulation (EU) 2016/279 and this Regulation.***

Amendment 27

Proposal for a regulation
Article 1

Text proposed by the Commission	*Amendment*
Article 1	Article 1
Subject matter	Subject matter
1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.	1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.
2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, which shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data.	2. This Regulation ensures, ***in accordance with Regulation (EU) 2016/679,*** 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.	3. The provisions of this Regulation complement Regulation (EU) 2016/679 by laying down ***necessary*** specific rules for the purposes mentioned in paragraphs 1 and 2. ***The provisions of Regulation (EU) 2016/679 shall apply unless this Regulation stipulates special provisions.***

Amendment 28

Proposal for a regulation
Article 2

Text proposed by the Commission	*Amendment*
Article 2	Article 2
Material Scope	Material Scope
1. This Regulation applies to the processing of electronic communications data carried out in connection with the	1. This Regulation applies to ***:***

provision and the use of electronic communications services and to information related to the terminal equipment of end-users.

(a) 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 terminal equipment of end-users***, regardless of whether a payment is required from the end user;***.

(b) information transmitted to, stored in, collected from, processed by or otherwise related to the terminal equipment of end-users, if not protected under Regulation (EU) 2016/679;

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;

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 ***pursuant to Article 2(2)(c) of Regulation (EU) 2016/679***;

(d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001].

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC[1], in particular of the liability rules of intermediary service providers in

(d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001].

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC[1], 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.

---

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1–16).

Articles 12 to 15 of that Directive.

5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.

---

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1–16).

Amendment 29

Proposal for a regulation
Article 3

Text proposed by the Commission	*Amendment*
Article 3	Article 3
Territorial scope and representative	Territorial scope and representative
1. This Regulation applies to:	1. This Regulation applies to ***the activities referred to in Article 2 where the end user is in the Union***:
(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.	
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.	2. Where the provider of an electronic communications service***, provider of a publicly available directory, software provider enabling electronic communications or person collecting information transmitted to, stored in, collected from, processed by or otherwise related to end-users terminal equipment*** is not established in the Union it shall designate in writing a representative in the

	Union ***pursuant to Article 27 of Regulation (EU) 2016/679***.
3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.	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.	4. The representative shall ***be authorised and provided with the relevant information by the provider it represents*** 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 ***the activities referred to in Article 2*** 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.	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 ***undertakes the activities referred to in Article 2*** from outside the Union to end-users in the Union.

Amendment 30

Proposal for a regulation
Article 4 – paragraph 3 – point c

Text proposed by the Commission	*Amendment*
c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;	c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including but not limited to, data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication; ***It includes data broadcast***

	or emitted by the terminal equipment to identify end-users' communications and/or terminal equipment in the network and enable it to connect to such network or to another device.

Amendment 31

Proposal for a regulation
Article 4 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
f) 'direct marketing communications' means any form of ***advertising***, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;	f) 'direct marketing communications' means any form of ***commercial communication***, 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.;

Amendment 32

Proposal for a regulation
Chapter 2 – title

Text proposed by the Commission	*Amendment*
PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION ***STORED IN*** THEIR TERMINAL EQUIPMENT	PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION ***PROCESSED BY AND RELATED TO*** THEIR TERMINAL EQUIPMENT

Amendment 33

Proposal for a regulation
Article 5

Text proposed by the Commission	*Amendment*
Article 5	Article 5

Confidentiality of electronic communications data	Confidentiality of electronic communications data
Confidentiality of electronic communications data	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.	***1.*** 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.
	1a. For the implementation of paragraph 1, providers of electronic communications networks and services shall take technical and organisational measures as defined in Article 32 of Regulation (EU) 2016/679. Additionally, to protect the integrity of terminal equipment and the safety, security and privacy of users, providers or electronic communications networks and services shall take appropriate measures based on the risk and on the state of the art to reasonably prevent the distribution, through their networks or services, of malicious software as referred to in Article 7 point a of Directive 2013/40/EU.
	1b. Confidentiality of electronic communications data shall also include terminal equipment and machine-to-machine communications when related to a user.

Amendment 34

Proposal for a regulation
Article 6

Text proposed by the Commission	*Amendment*
Article 6	Article 6

Permitted processing of electronic communications data	Permitted processing of electronic communications data
Permitted processing of electronic communications data	***Lawful*** processing of electronic communications data
1. Providers of electronic communications networks and services may process electronic communications data if:	1. Providers of electronic communications networks and services may process electronic communications data ***only***:
(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or	(a) if it is ***technically strictly*** necessary to achieve the transmission of the communication, for the duration necessary for that purpose ***and the data is stored in a binary format***; or
(b) it is necessary to maintain or restore ***the*** security of electronic communications networks ***and*** services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose**.**	(b) if it is ***technically strictly*** necessary to maintain or restore ***availability, integrity, confidentiality and*** security of ***the respective*** electronic communications networks ***or*** services, or ***to*** detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose***; or***
	(ba) where such processing produces effects solely in relation to the user who requested the service and does not adversely affect the fundamental rights of other users, where the user has given his or her consent to the processing of his or her electronic communications data, and to the extent that the purpose concerned could not be fulfilled without the processing of such metadata.
2. Providers of electronic communications services may process electronic communications metadata if:	2. Providers of electronic communications services may process electronic communications metadata ***only***:
(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[1] for the duration necessary for that purpose; or	(a) if it is ***strictly*** necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120[1] for the duration ***technically*** necessary for that purpose; or
(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic	(b) if it is ***strictly*** necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive ***unlawful*** use of, or subscription to,

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***.

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.

electronic communications services; or

(c) ***after receiving all relevant information about the intended processing in clear and easily understandable language, provided separately from the terms and conditions of the provider,*** the end-user concerned has given his or her ***prior*** 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 ***without the*** processing ***of such metadata***.

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 ***requested by the*** end-user, if the end-user concerned ***has*** given ***his or her prior*** 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 ***by the provider, and the consent has not been a condition to access or use a service***; or

(b) if all end-users concerned have given their ***prior*** 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.

3a. For the provision of a service explicitly requested by an end-user of an electronic communications service for his/her purely individual or individual work-related usage, the provider of the electronic communications service may process electronic communications data solely for the provision of the explicitly

	requested service and without the consent of all users only where such requested processing produces effects solely in relation to the end-user who requested the service and does not adversely affect the fundamental rights of another user or users. Such a specific consent by the end-user shall preclude the provider from processing these data for any other purpose.
[1] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).	[1] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).

Amendment 35

Proposal for a regulation
Article 7

Text proposed by the Commission	*Amendment*
Article 7	Article 7
Storage and erasure of electronic communications data	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)	1. Without prejudice to point (b) of Article 6(1)***,*** points (a) ***and (c) of Article 6(2) and points (a)*** and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications 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 ***specific other third*** party entrusted by them to record, store or otherwise

2016/679.	process such data in accordance with Regulation (EU) 2016/679.
2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.	2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.
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 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.	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 data which is strictly necessary*** 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.

Amendment 36

Proposal for a regulation
Article 8

Text proposed by the Commission	*Amendment*
Article 8	Article 8
Protection of information stored in and related to end-users' terminal equipment	Protection of information stored in, related to ***and processed by*** end-users' terminal equipment
1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:	1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, ***or making information available through the terminal equipment,*** including ***information*** about ***or generated by*** its software and hardware, ***and any other electronic communications data identifying end-users,*** other than by the end-user concerned shall be prohibited, except on the following grounds:
(a) it is necessary for the sole purpose of carrying out the transmission of an	(a) it is ***strictly*** necessary for the sole purpose of carrying out the transmission of

electronic communication over an electronic communications network; or	an electronic communication over an electronic communications network ***whereby the data shall be stored in a binary format***; or
(b) the end-user ***has*** given ***his or her*** consent; ***or***	(b) ***all*** the end-user ***have*** given ***their prior and specific*** consent***, which shall not be mandatory to access the service***;
(c) it is necessary for providing an information society service requested by the end-user; or	(c) it is ***strictly*** necessary for providing an information society service requested by the end-user***, for the duration necessary for that provision of the service, provided that the provision of that specific service cannot be fulfilled without the processing of such content by the provider***; or
(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society ***service requested by*** the end-user.	(d) if it is ***strictly*** necessary for web audience measuring ***of the information society service requested by the end-user***, provided that such measurement is carried out by the provider***, or on behalf*** of the ***provider, on by an independent web analytics agency acting in the public interest or for scientific purpose; and provided furthermore that no personal data is made accessible to any other party and that such web audience measurement does not entail tracking of the end-user across different*** information society ***services and respects the fundamental rights of*** the end-user.
	(da) the data is deleted without any undue delay once the purpose of the collection ceases to exists.
	(daa) it is strictly technically necessary for a security update, provided that:
	(i) such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;
	(ii) the user is informed in advance each time such an update is being installed; and
	(iii) the user has the possibility to postpone or turn off the automatic installation of such updates;

	(db) if this is strictly necessary for the personalisation of electronic communication services provided to and expressly requested by end-users.
	Points a, c and d shall be limited to situations that involve no, or only very restrictive, intrusion of privacy or other fundamental rights.
	No user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that the end-user does not provide consent as set out in point (b) of Article 8(1) or point (b) of Article 8(2) for processing any data that is not strictly necessary for the functionality requested by the end-user.
2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:	2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:
(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or	(a) it is done exclusively in order to, for the time necessary for, and for the ***sole*** purpose of establishing a connection ***requested by the end-user***; or
	(aa) the end-user has given his or her consent; or
	(ab) the data are anonymised and the risks are adequately mitigated.
(b) a clear and ***prominent notice is displayed informing of,*** at least***, the modalities of the collection, its*** purpose, the person responsible for it and ***the*** other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected***, as well as any measure the end-user of the terminal equipment can take to stop or minimise the*** collection.	(b) ***all relevant information about the intended processing is provided in*** a clear and ***reader-friendly notice, provided separately from the terms and conditions of the provider, setting out*** at least ***the details of how the information will be collected, the*** purpose ***of collection***, the person responsible for it and other information required under Article 13 of Regulation (EU) 2016/679***,*** where personal data are collected***. 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.
The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.
	2a. For the purpose of point (ab) of paragraph 2, the following controls shall be implemented to mitigate the risks:
	(a) the purpose of the data collection from the terminal equipment shall be restricted to mere statistical counting;
	(b) the tracking shall be limited in time and space to the extent strictly necessary for this purpose;
	(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and
	(d) the end-users shall be given effective opt-out possibilities.
3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.	4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.

Amendment 37

Proposal for a regulation
Article 9

Text proposed by the Commission	*Amendment*
Article 9	Article 9
Consent	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.	1. The definition of and conditions for consent provided for under Articles 4(11) and 7 ***(1), (2) and (3)*** of Regulation (EU) 2016/679/EU shall apply.
2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using ***the appropriate*** technical ***settings of a software application enabling access to the internet***.	2. Without prejudice to paragraph 1, where technically possible and feasible, ***in particular*** for the purposes of point (b) of Article 8(1), consent may be expressed by using technical ***specifications of electronic communications services. When such technical specifications are used by the end-user, they shall be binding on, and enforceable against, any other party***.
3. End-users who have ***consented*** to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 ***and*** be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.	3. End-users who have ***given their consent*** 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)***, point (b) of Article 8(1) and point (aa) of Article 8(2)*** shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679***. It shall be as easy to withdraw as to give consent and, furthermore, the end-user should*** be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.

Amendment 38

Proposal for a regulation
Article 10

Text proposed by the Commission	*Amendment*
Article 10	Article 10
Information and options for privacy settings to be provided	Information and options for privacy settings to be provided ***- privacy by design and by default***

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

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall:

1-a. 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.

1a. By default, offer privacy protective settings to prevent other parties from storing information on the terminal equipment of a user and from processing information already stored on that equipment;

1b. Upon installation, inform and offer the user the possibility to change or confirm the privacy settings options defined in point (a) by requiring the user's consent to a setting;

1c. Make the setting defined in points (a) and (b) easily accessible during the use of the software; and

1d. Offer the user the possibility to express specific consent through the settings after the installation of the software.

2. ***Upon installation, the software*** shall ***inform the end-user*** about the privacy settings ***options and, to continue with the installation, require the end-user to consent to a setting***.

2. ***For the purpose of points (a) and (b) of paragraph 1, the settings*** shall ***include a signal which is sent to the other parties to inform them*** about the ***user's*** privacy settings***. These settings shall be binding on, and enforceable against, any other party***.

The European Data Protection Board shall issue guidelines to determine which technical specifications and signalling methods fulfil the conditions for consent and objection pursuant to paragraph 1 points (a) and (b).

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

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.	than 25 August 2018.

Amendment 39

Proposal for a regulation
Article 10 a (new)

Text proposed by the Commission	*Amendment*
	Article 10a
	This software must ensure that the consent given by an end-user in accordance with point (b) of Article 8(1) takes precedence over the parameters chosen when the software was installed.
	The software must not block data processing which is legally authorised in accordance with Article 8(1)(a), (b), (c) or (d) or (2)(a), whatever the browser settings.

Amendment 40

Proposal for a regulation
Article 11

Text proposed by the Commission	*Amendment*
Article 11	Article 11
Restrictions	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 Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of	1. Union or Member State law ***to which the provider is subject*** 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 ***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*** and is a necessary, appropriate and proportionate measure in a democratic society to

official authority for such interests.	safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.
	1a In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least pursuant to Article 23(2) of Regulation (EU) 2016/679, where relevant.
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.	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. ***Providers shall respond to requests for access in accordance with the legal requirements where the service provider has its main establishment under Regulation (EU) 2016/679. For requests from a Member State where the service provider is not established, cross-border mechanisms for requests under mutual legal assistance conventions or Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters shall be followed. Without prejudice to any requirements under Member State law to provide information to competent law enforcement authorities, 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.

Amendment 41

Proposal for a regulation
Article 15

Text proposed by the Commission	*Amendment*
Article 15	Article 15
Publicly available directories	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.	1. The providers of publicly available directories ***or the electronic communication service providers*** shall obtain ***prior*** consent of end-users who are natural persons to include their personal data in the directory ***to organize personal*** data per ***categories***, to the extent that such data are relevant for the purpose of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data ***or to withdraw their consent at any time***.
2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.	2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to 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.	3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.
4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.	4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.

Amendment 42

Proposal for a regulation
Article 16– paragraph 1

Text proposed by the Commission	*Amendment*
(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.	(1) ***The use by*** natural or legal persons ***of electronic communications services, including voice-to-voice calls, automated calling and communications systems, including semi-automated systems that connect the call person to an individual, faxes, e-mail or other*** use ***of*** electronic communications services for the purposes of ***presenting unsolicited or*** direct marketing communications to end-users***, shall be allowed only in respect of end-users*** who have given their ***prior*** consent.

Amendment 43

Proposal for a regulation
Article 16– paragraph 2

Text proposed by the Commission	*Amendment*
(2) Where a natural or legal person obtains electronic contact details for ***e-mail*** from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.	(2) Where a natural or legal person obtains electronic contact details for ***electronic mail*** from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services ***for a period of no more than 12 months*** only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The ***customer shall be informed about the*** right to object ***and*** shall be given ***an easy way to exercise it*** at the time of collection and each time a message is sent.

Amendment 44

Proposal for a regulation
Article 16 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
a) present the identity of a line on which they can be contacted; ***or***	a) present the identity of a line on which they can be contacted; ***and***

Amendment 45

Proposal for a regulation
Article 16 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	(3a) Unsolicited marketing communications shall be clearly recognisable as such and shall indicate the identity of the legal or natural person transmitting the communication or on behalf of whom the communication is transmitted. Such communications shall provide the necessary information for recipients to exercise their right to refuse further written or oral marketing messages.

Amendment 46

Proposal for a regulation
Article 16 – paragraph 4

Text proposed by the Commission	*Amendment*
(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.	***deleted***

Amendment 47

Proposal for a regulation
Article 16 – paragraph 6

Text proposed by the Commission	*Amendment*
(6) Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in ***an*** easy ***manner***, to receiving further marketing communications.	(6) Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent ***or object***, in ***a manner that is as*** easy ***as giving the consent and free of charge***, to receiving further marketing communications.

Amendment 48

Proposal for a regulation
Article 17

Text proposed by the Commission	*Amendment*
Article 17	Article 17
Information about detected security risks	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.***	In the case of a particular risk ***or a significant threat*** that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall ***comply with the security obligations provided for in Articles 32 to 34 of Regulation (EU) 2016/679 and in Article 40 of the Directive establishing the European Electronic Communications Code.***

Amendment 49

Proposal for a regulation
Article 21

Text proposed by the Commission	*Amendment*
Article 21	Article 21

Remedies	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.	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 ***and 80*** 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.	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.

Amendment 50

Proposal for a regulation
Article 22 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	Article 82 of Regulation (EU) No 2016/679 ***shall apply***.

Justification

Article 82 of Regulation (EU) No 2016/679 already regulates the issue of liability and the right to compensation. The article inserted in Article 22 of the proposal for a regulation extends and specifies Article 82 of Regulation (EU) No 2016/679 and makes this proposal lex specialis.

Amendment 51

Proposal for a regulation
Article 23

Text proposed by the Commission	*Amendment*
Article 23	***deleted***
General conditions for imposing administrative fines	
(1) For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation.	
(2) Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:	
(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;	
(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;	
(c) the obligations of the providers of publicly available directories pursuant to Article 15;	
(c) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.	
(3) Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total	

worldwide annual turnover of the preceding financial year, whichever is higher.

(4) Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17.

(5) Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

(6) Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

(7) The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

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

Justification

Article 83 of Regulation (EU) No 2016/679 regulates the general preconditions for the imposition of fines. The specification here amends Article 83 of Regulation (EU) No 2016/679 and creates a dual regime. This dual structure would hamper the correct application of the law by supervisory authorities and courts and lead to unfair treatment.

Amendment 52

Proposal for a regulation
Article 23 a (new)

Text proposed by the Commission	*Amendment*
	Article 23a
	Article 83 of Regulation (EU) No 2016/679 shall apply;

Justification

Article 83 of Regulation (EU) No 2016/679 regulates the general preconditions for the imposition of fines. The specification here amends Article 83 of Regulation (EU) No 2016/679 and creates a dual regime. This dual structure would hamper the correct application of the law by supervisory authorities and courts and lead to unfair treatment.

Amendment 53

Proposal for a regulation
Article 24

Text proposed by the Commission	*Amendment*
Article 24	***deleted***
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.	

Justification

Article 84 of Regulation (EU) No 2016/679 regulates penalties. The specification here amends Article 84 of Regulation (EU) No 2016/679 and creates a dual regime. This dual structure would hamper the correct application of the law by supervisory authorities and courts and lead to unfair treatment.

Amendment 54

Proposal for a regulation
Article 24 a (new)

Text proposed by the Commission	*Amendment*
	Article 24a
	Article 84 of Regulation (EU) No 2016/679 shall apply.

Justification

Article 84 of Regulation (EU) No 2016/679 regulates penalties. The specification here amends Article 84 of Regulation (EU) No 2016/679 and creates a dual regime. This dual structure would hamper the correct application of the law by supervisory authorities and courts and lead to unfair treatment.

Amendment 55

Proposal for a regulation
Article 25 – paragraph 2

Text proposed by the Commission	*Amendment*
(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	(2) The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for ***5 years*** from [the date of entering into force of this Regulation].

Regulation].

Amendment 56

Proposal for a regulation
Article 28 – paragraph 1

Text proposed by the Commission	*Amendment*
By 1 January 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.	***Six months before the entry into force of this Regulation*** at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	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)
References	COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)
Committee responsible Date announced in plenary	LIBE 16.2.2017
Opinion by Date announced in plenary	JURI 16.2.2017
Rapporteur Date appointed	Axel Voss 28.2.2017
Discussed in committee	29.5.2017 19.6.2017 7.9.2017
Date adopted	2.10.2017
Result of final vote	+: 11 –: 10 0: 1
Members present for the final vote	Max Andersson, Joëlle Bergeron, Marie-Christine Boutonnet, Jean-Marie Cavada, Mary Honeyball, Sylvia-Yvonne Kaufmann, Gilles Lebreton, Jiří Maštálka, Emil Radev, Julia Reda, Evelyn Regner, Pavel Svoboda, József Szájer, Axel Voss, Francis Zammit Dimech, Tadeusz Zwiefka
Substitutes present for the final vote	Isabella Adinolfi, Angel Dzhambazki, Jens Rohde, Virginie Rozière, Tiemo Wölken
Substitutes under Rule 200(2) present for the final vote	Arne Lietz

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

11	+
ALDE	Jean-Marie Cavada, Jens Rohde
GUE/NGL	Jiří Maštálka
S&D	Mary Honeyball, Sylvia-Yvonne Kaufmann, Arne Lietz, Evelyn Regner, Virginie Rozière, Tiemo Wölken
VERTS/ALE	Max Andersson, Julia Reda

10	-
ECR	Angel Dzhambazki
EFDD	Joëlle Bergeron
ENF	Marie-Christine Boutonnet, Gilles Lebreton
PPE	Emil Radev, Pavel Svoboda, József Szájer, Axel Voss, Francis Zammit Dimech, Tadeusz Zwiefka

1	0
EFDD	Isabella Adinolfi

Key to symbols:
+ : in favour
- : against
0 : abstention