



Plenary sitting

A8-0324/2017

20.10.2017

*****I**
REPORT

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))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Marju Lauristin

Symbols for procedures

- * Consultation procedure
- *** Consent procedure
- ***I Ordinary legislative procedure (first reading)
- ***II Ordinary legislative procedure (second reading)
- ***III Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

Amendments by Parliament set out in two columns

Deletions are indicated in ***bold italics*** in the left-hand column. Replacements are indicated in ***bold italics*** in both columns. New text is indicated in ***bold italics*** in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

Amendments by Parliament in the form of a consolidated text

New text is highlighted in ***bold italics***. Deletions are indicated using either the **■** symbol or ~~strikeout~~. Replacements are indicated by highlighting the new text in ***bold italics*** and by deleting or striking out the text that has been replaced.

By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.

CONTENTS

	Page
DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION.....	4
EXPLANATORY STATEMENT.....	90
ANNEX: LIST OF ENTITIES FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT	95
OPINION OF THE COMMITTEE ON INDUSTRY, RESEARCH AND ENERGY	98
OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION	143
OPINION OF THE COMMITTEE ON LEGAL AFFAIRS	191
PROCEDURE – COMMITTEE RESPONSIBLE.....	244
FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE.....	245

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

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))

(Ordinary legislative procedure: first reading)

The European Parliament,

- having regard to the Commission proposal to Parliament and the Council (COM(2017)0010),
 - having regard to Article 294(2) and Articles 16 and 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C8-0009/2017),
 - having regard to Article 294(3) of the Treaty on the Functioning of the European Union,
 - having regard to the contributions submitted by the Czech Chamber of Deputies, the Czech Senate, the German Bundesrat, the Spanish Parliament, the Italian Chamber of Deputies, the Netherlands Senate and the Portuguese Parliament on the draft legislative act,
 - having regard to the opinion of the European Economic and Social Committee¹;
 - having regard to Rules 59 of its Rules of Procedure,
 - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Industry, Research and Energy, the Committee on the Internal Market and Consumer Protection and the Committee on Legal Affairs (A8-0324/2017),
1. Adopts its position at first reading hereinafter set out;
 2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;
 3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

¹ OJ C 345, 13.10.2017, p. 138.

Amendment 1

Proposal for a regulation

Recital 1

Text proposed by the Commission

(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.

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 *communicating* parties. The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e-mail, internet phone calls and *inter-personal* messaging provided through social media. *It should also apply when the confidentiality of electronic communications and the privacy of the physical environment converge, i.e. where terminal devices for electronic communications can also listen into their physical environment or use other input channels such as Bluetooth signalling or movement sensors.*

Amendment 2

Proposal for a regulation

Recital 2

Text proposed by the Commission

(2) The content of electronic communications may reveal highly

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.

Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc.

sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment.

Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communications, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc. ***Metadata can also be processed and analysed much easier than content, as it is already brought into a structured and standardised format. 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 4

Text proposed by the Commission

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

Amendment

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

communications data *may include* personal data as defined in Regulation (EU) 2016/679.

communications data *are generally* personal data as defined in Regulation (EU) 2016/679.

Amendment 4

Proposal for a regulation Recital 5

Text proposed by the Commission

(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.

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. ***On the contrary, it aims to provide additional and complementary safeguards take into account the need for additional protection as regards the confidentiality of communications.*** Processing of electronic communications data should only be permitted in accordance with, this Regulation.

Amendment 5

Proposal for a regulation Recital 6

Text proposed by the Commission

(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council²² 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

Amendment

(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council²² 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.

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 6

Proposal for a regulation

Recital 7

Text proposed by the Commission

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

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 **users**. 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).

Amendment

(7) The **European Data Protection Board** should, **where necessary, issue guidance and opinions**, within the limits of this Regulation, to maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. **Cooperation and consistency between Member States, in particular between national Data Protection Authorities, is essential to** maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.

Amendment 7

Proposal for a regulation

Recital 8

Text proposed by the Commission

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

Amendment

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

Amendment 8

Proposal for a regulation

Recital 9

Text proposed by the Commission

(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.

Amendment

(9) This Regulation should apply to electronic communications data processed in connection with the ***offering*** 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. For the purpose of this Regulation, where the provider of an electronic communications service is not established in the Union, it***

should designate, in writing, a representative in the Union.

Amendment 9

Proposal for a regulation

Recital 11

Text proposed by the Commission

(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 Code²⁴]. 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.***

²⁴ *Commission proposal for a Directive of the European Parliament and of the*

Amendment

(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services, ***also known as “over-the-top-services” (OTTs). This Regulation aims at ensuring*** an effective and equal protection of end-users when using functionally equivalent services, ***so as to ensure the confidentiality of their communications, irrespective of the technological medium chosen. It does*** not only ***cover*** 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.

Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

Amendment 10

Proposal for a regulation

Recital 12

Text proposed by the Commission

Amendment

(12) *Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.*

deleted

Amendment 11

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

(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*.

internet access via wireless networks accessible by anyone in public and semi-private spaces such as *wireless internet access points* situated at different places within a city, *for example* department stores, shopping malls, hospitals, *airports, hotels and restaurants. Those access points might require a log in or provide a password and might be provided also by public administrations, including Union bodies and agencies.* To the extent that those communications networks are provided to *users*, the confidentiality of the communications transmitted through such networks should be protected. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. *This Regulation should also apply to closed social media profiles and groups that the users have restricted or defined as private.* In contrast, this Regulation should not apply to closed groups of end-users such as corporate *intranet* networks, access to which is limited to members of *an organisation. The mere requirement of a password should not be considered as providing access to a closed group of end-users if the access to the service as a whole is provided to an undefined group of end-users.*

Amendment 12

Proposal for a regulation

Recital 14

Text proposed by the Commission

(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

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 *a 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 data necessary to identify users' terminal equipment and data emitted by terminal equipment when searching for access points or other equipment.*** Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content. ***The exclusion of services providing "content transmitted using electronic communications networks" from the definition of "electronic communications service" in Article 4 of this Regulation does not mean that service providers who offer both electronic communications services and content services are outside the scope of the provisions of the Regulation which applies to the providers of electronic communications services.***

Amendment 13

Proposal for a regulation Recital 14 a (new)

(14 a) Modern electronic communications services, including the Internet and the OTT services that run on top of it, function on the basis of a protocol stack. Each protocol defines content (also called payload), a header and sometimes a trailer. Any higher protocol in the stack would be encapsulated in the content part of a lower level protocol. For example, A TCP segment would be in the content part of an IP packet, whose header would include the source and destination IP addresses between which the IP packet should be routed. TCP segments could contain an SMTP message in their content part, i.e. an e-mail. At the SMTP protocol level, the header would notably contain the sender and receiver email addresses and the content part would contain the message itself. In practice, the header and the trailer of a protocol message correspond to metadata for the given protocol. This means that the metadata on one protocol layer will be content for the lower layers encapsulating the information. Where this Regulation lays down different rules for the processing of content and metadata, this should be understood specifically for the considered electronic communications service and the protocol layer it is operating on. For an Internet service provider, for example, the subject, the sender, the recipient and the body of an email will be altogether considered as content of the IP packets routed by it. However regarding an e-mail provider, only the subject and the body of the email will be considered as content, whereas the recipient and the sender will be considered as metadata. This separation of protocol layers is crucial for maintaining the neutrality of the electronic communications services (net neutrality), which is protected under Regulation (EU) 2015/2120.

Amendment 14

Proposal for a regulation

Recital 15

Text proposed by the Commission

(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

Amendment

(15) Electronic communications should be treated as confidential. This means that any interference with the transmission of electronic communications, 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. ***When the processing is allowed under any exception to the prohibitions under this Regulation, any other processing on the basis of Article 6 of Regulation (EU) 2016/679 should be considered as prohibited, including processing for another purpose on the basis of Article 6 paragraph 4 of that Regulation. This should not prevent requesting additional consent for new processing operations.*** The prohibition of interception of communications should apply ***also*** during their conveyance. ***For non-real-time electronic communications such as email or messaging, the transmission starts with the submission of the content for delivery and finishes with the receipt of the content of the electronic communication by the service provider of the intended recipient.*** Interception of electronic communications 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 **user** concerned. As technology evolves, the technical ways to

the *end-users'* consent.

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 *user* profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, ***and analysis of users' traffic data, including browsing habits without the users' consent.***

Amendment 15

Proposal for a regulation

Recital 16

Text proposed by the Commission

(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.

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. ***It should not prohibit the processing of*** electronic communications ***data by public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), providers*** of electronic communications ***networks and services and by providers of security technologies and services, in compliance with Regulation 2016/679 and to the extent strictly necessary and proportionate for the sole purposes of ensuring network and information security, [i.e. preservation of availability, integrity], and confidentiality of information, and ensuring*** the security of the ***related services offered by, or accessible via, those networks and systems. This could, for example, include preventing unauthorised access to***

electronic communications *networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communications systems, security* services, checking security threats such as the presence of malware, *spam or to check against DDoS attacks*, or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc. *Such processing could be carried out by another party which acts as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service.*

Amendment 16

Proposal for a regulation Recital 17

Text proposed by the Commission

(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

Amendment

(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. However, *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. *This* Regulation should require providers of electronic communications services to obtain *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. Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and

communications services should not be considered as metadata. *Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure.* Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.

purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.

Amendment 17

Proposal for a regulation Recital 17 a (new)

Text proposed by the Commission

Amendment

(17 a) Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of

data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure.

Amendment 18

Proposal for a regulation Recital 18

Text proposed by the Commission

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

Amendment

(18) ***The user or end-user*** may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements. For the purposes of this Regulation, consent of a ***user***, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. Basic broadband internet access and voice communications services are to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment. ***Consent should not be***

unable to refuse or withdraw consent without detriment.

considered as freely given if it is required to access any service or obtained through repetitive requests. In order to prevent such abusive requests, users should be able to order service providers to remember their choice not to consent and to adhere to technical specifications signalling not to consent, withdrawal of consent, or an objection.

Amendment 19

Proposal for a regulation Recital 19

Text proposed by the Commission

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any ***interference with the*** content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the ***end-users*** concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. ***Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the***

Amendment

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any ***processing of content data*** of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the ***users*** concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always ***carry out an impact assessment as provided for in Regulation (EU) 2016/679 and if necessary under that Regulation,*** consult the supervisory authority prior to the processing. After electronic

processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the *end-user* and received by the intended *end-user or end-users*, it may be recorded or stored by the *end-user, end-users* or by a third party entrusted by them to record or store such data. Any processing of such *data* must comply with Regulation (EU) 2016/679.

communications content has been sent by the *user* and received by the intended *user or users*, it may be recorded or stored by the *user, users* or by a third party entrusted by them to record or store such data, *which could be the electronic communications service provider.* Any processing of such *stored communications data where the data is stored on behalf of the user must comply with this Regulation. The user may further process the data and if it contains personal data,* must comply with Regulation (EU) 2016/679.

Amendment 20

Proposal for a regulation Recital 19 a (new)

Text proposed by the Commission

Amendment

(19 a) It should be possible to process electronic communications data for the purposes of providing services explicitly requested by a user for personal or personal work-related purposes such as search or keyword indexing functionality, virtual assistants, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools by persons with disabilities. This should be possible without the consent of all users but may take place with the consent of the user requesting the service. Such consent also precludes the provider from processing those data for other purposes.

Amendment 21

Proposal for a regulation Recital 19 b (new)

(19 b) Interference with the confidentiality of metadata or interference with the protection of information stored in and related to end-users' terminal equipment can only be regarded to be lawful where it is strictly necessary and proportionate to protect an interest which is essential for the life of the data subject or that of another natural person. Such interference based on the vital interest of another natural person should take place only in a specific case and where the processing cannot be manifestly based on another legal basis.

Amendment 22

Proposal for a regulation Recital 20

Text proposed by the Commission

(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

Amendment

(20) Terminal equipment of ***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 ***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 ***very sensitive data*** that may reveal details of ***the behaviour, psychological features,*** emotional ***condition and*** political ***and*** social ***preferences of an individual,*** including the content of communications, pictures, the location of individuals by accessing the GPS capabilities ***of the device,*** contact lists, and other information

requires enhanced privacy protection. ***Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities.*** Information related to the *end-user's* device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these *end-users*. Techniques that surreptitiously monitor the actions of *end-users*, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the *end-users'* terminal equipment pose a serious threat to the privacy of *end-users*. Therefore, any such interference with the *end-user's* terminal equipment should be allowed only with the *end-user's* consent and for specific and transparent purposes.

already stored in the device, the information related to such equipment requires enhanced privacy protection. Information related to the 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 *users*. ***Furthermore, so-called spyware, web bugs, hidden identifiers and unwanted tracking tools can enter users' terminal equipment without their knowledge in order to gain access to information or to store hidden information, to process data and use input and output functionalities such as sensors, and to trace the activities.*** Techniques that surreptitiously monitor the actions of *users*, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the *users'* terminal equipment pose a serious threat to the privacy of *users*. Therefore, any such interference with the *user's* terminal equipment should be allowed only with the *user's* consent and for specific and transparent purposes. ***Users should receive all relevant information about the intended processing in clear and easily understandable language. Such information should be provided separately from the terms and conditions of the service.***

Amendment 23

Proposal for a regulation Recital 21

Text proposed by the Commission

(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access

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 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.

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 **authorising** 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 **user**. This may include the storing of **information (such as cookies and other identifiers)** 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. **Such techniques, if implemented with appropriate privacy safeguards**, can also be a legitimate and useful tool, for example, in measuring web traffic to a website. **Such measuring implies that the result of processing is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.** Information society providers **could** engage in configuration checking **in order** to provide the service in compliance with the **user's** settings and the mere logging **revealing** the fact that the user's device is unable to receive content requested by the **user**, should not constitute **illegitimate** access to such a device, or use of the device processing capabilities **for which consent is required**.

Amendment 24

Proposal for a regulation

Recital 22

Text proposed by the Commission

(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

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 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.

techniques, *users* are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, *users* are overloaded with requests to provide consent. ***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.*** 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 ***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 *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, ***or applications or operating systems*** may be used as ***the executor of a user's choices***, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

Amendment 25

Proposal for a regulation

Recital 23

Text proposed by the Commission

(23) The principles of data protection by design and by default *were* codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to ‘accept all cookies’. Therefore providers of software *enabling the retrieval and presentation of information on the internet should have an obligation to* configure the software so that *it offers the option to prevent third parties from* storing information on the terminal equipment; *this is often presented as ‘reject third party cookies’*. End-users *should be offered a set of privacy setting options, ranging from higher (for example, ‘never accept cookies’) to lower* (for example, ‘always accept cookies’) *and intermediate* (for example, ‘reject third party cookies’ or ‘only accept first party cookies’). Such privacy settings should be presented in a an easily visible and intelligible manner.

Amendment

(23) The principles of data protection by design and by default *are* 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 *permitting electronic communications (such as browsers, operating systems and communication apps), irrespective of whether the software is obtained separately or bundled with hardware, shall* configure the software so that *privacy is protected, the cross-domain tracking and the* storing of information on the terminal equipment *by third parties is prohibited by default. In addition, providers of such software are required to offer sufficiently granular options to consent to each distinct category of purposes. These distinct categories include, at least, the following categories: (i) tracking for commercial purposes or for direct marketing for non-commercial purposes (behavioural advertising); (ii) tracking for personalised content; (iii) tracking for analytical purposes; (iv) tracking of location data; (v) providing personal data to third parties (including providing unique identifiers to match with personal data held by third parties) No consent is required for information that is collected from end-users’ terminal equipment when it is strictly necessary for providing an information society service requested by the end-user, for example in order to adapt the screen size to the device, or to remember items in a shopping basket. Web browsers, operating systems and communication apps should allow the*

end-user to consent to cookies or other information that is stored on, or read from terminal equipment (including the browser on that equipment) by a specific website or originator even when the general settings prevent the interference and vice versa. With regard to a specific party, web browsers and communication apps should also allow users to separately consent to internet-wide tracking. Privacy settings should also include options to allow the user to decide for example, whether multimedia players, interactive programming language viewers, 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 and intelligible manner, and at the moment of installation or first use, users should be informed about the possibility to change the default privacy settings among the various options. Information provided should not dissuade users from selecting higher privacy settings and should include relevant information about the risks associated to allowing cross-domain trackers, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising or sharing with more third parties. Software manufacturers should be required to provide easy ways for users to change the privacy settings at any time during use and to allow the user to make exceptions for or to specify for such services websites trackers and cookies are always or never allowed.

Amendment 26

Proposal for a regulation Recital 24

(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 27

Proposal for a regulation Recital 25

(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to **end-users**, for example when they enter stores, with **personalized** offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should **display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to**

(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 **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 **either obtain the 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 28

Proposal for a regulation

Recital 26

Text proposed by the Commission

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

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 Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights.

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 29

Proposal for a regulation Recital 26 a (new)

Text proposed by the Commission

Amendment

(26 a) In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design. Member States should not impose any obligation on encryption providers, on providers of electronic communications services or on any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of “backdoors”.

Amendment 30

Proposal for a regulation Recital 30

Text proposed by the Commission

Amendment

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person requires

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person requires

that *end-users that are natural persons* are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.

that *users* are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory. ***The consent should be collected by the electronic communications service provider at the moment of signing the contract for such service. Natural persons acting in a professional capacity, such as independent professionals, operators of small businesses or freelancers, shall be equated with legal persons, as regards their data related to their professional capacity.***

Amendment 31

Proposal for a regulation

Recital 31

Text proposed by the Commission

(31) If *end-users that are natural persons* give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, providers of *publicly available directories* should inform the *end-users* of the purposes of the directory and of the search functions of the directory before including them in that directory. *End-users* should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the *end-user's* contact details can be searched should not necessarily be the same.

Amendment

(31) If *users* give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, *electronic communications service* providers should inform the *users* of the purposes of the directory and of the search functions of the directory before including them in that directory. *Users* should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the *user's* contact details can be searched should not necessarily be the same. ***The providers or publicly available directories shall provide information about the search functions, as well as if new options and functions of the directories are available in the***

publicly available directories and provide the users the option to disable such functions.

Amendment 32

Proposal for a regulation Recital 32

Text proposed by the Commission

(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.

Amendment

(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services, ***regardless of the form it takes***. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.

Amendment 33

Proposal for a regulation Recital 33

Text proposed by the Commission

(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,

Amendment

(33) Safeguards should be provided to protect end-users against unsolicited communications ***or*** direct marketing, 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 ***communications systems, semi-automated*** systems, instant messaging applications,

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.

faxes, e-mails, 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 *and* 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 *high* level of protection for all *end-users* 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 *other* 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.

Amendment 34

Proposal for a regulation

Recital 36

Text proposed by the Commission

(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on end-users. Member States *should therefore be able* to establish and or maintain national systems only allowing such calls to end-users who have not objected.

Amendment

(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communications systems, given that they are more costly for the sender and impose no financial costs on end-users, *justify the obligation for* Member States to establish and or maintain national systems only allowing such calls to end-users who have not objected.

Amendment 35

Proposal for a regulation Recital 37

Text proposed by the Commission

(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.

Amendment

(37) Service providers who offer electronic communications services should ***process electronic communications data in such a way as to prevent unauthorised processing, including access, or alteration. They should ensure that such unauthorised access or alteration can be detected, and also ensure that electronic communications data are protected by using state-of-the art software and cryptographic methods including encryption technologies. Service providers should also*** inform 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. ***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 36

Proposal for a regulation Recital 38

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

(38) To ensure full consistency with Regulation (EU) 2016/679, The enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. ***Where more than one supervisory authority is established in a Member State, such authorities should cooperate with each other. They should also cooperate with the authorities appointed to enforce the European Electronic Communications Code and other relevant enforcement authorities, such as the authorities tasked with consumer protection.*** Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.

Amendment 37

Proposal for a regulation Recital 38 a (new)

(38a) The enforcement of the provisions of this Regulation often requires cooperation between the national supervisory authorities of two or more Member States, for example in combating interferences with the confidentiality of the terminal equipment. In order to ensure a smooth and rapid cooperation in such cases, the procedures of the cooperation and consistency mechanism established under Regulation 2016/679/EU should apply to Chapter II of this Regulation. Therefore, the European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, in particular by issuing opinions in the context of the consistency mechanisms or by adopting binding decisions in the context of dispute resolution as provided in Article 65 of Regulation 2016/679/EU, as regards Chapter II of this Regulation.

Amendment 38

Proposal for a regulation Recital 39

Text proposed by the Commission

(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their

Amendment

(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks, ***including adopting binding decisions***, set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, ***including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers***, without prejudice to the powers of prosecutorial authorities under Member

supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.

State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.

Amendment 39

Proposal for a regulation

Recital 41

Text proposed by the Commission

(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to ***the protection*** of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the ***end-user*** of the terminal equipment can take to minimise the collection. ***Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems.*** It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016²⁵. In particular, to ensure equal participation in the preparation of delegated acts, the

Amendment

(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons ***in the provision and use of electronic communications services*** and in particular their right to ***respect of their private life and communications with regard to the processing*** of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the ***user*** of the terminal equipment can take to minimise the collection. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016²⁵. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council

European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. *For instance, implementing measures* are necessary to specify a code to identify direct marketing calls including those made through automated calling and communications systems. *They are also necessary to establish the procedures and circumstances to override the elimination of the presentation of the calling line identification on a temporary basis where users request the tracing of malicious or nuisance calls* Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

²⁵ Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016 (OJ L 123, 12.5.2016, p. 1–14).

²⁵ Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016 (OJ L 123, 12.5.2016, p. 1–14).

Amendment 40

Proposal for a regulation Article 2 – paragraph 1

Text proposed by the Commission

1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.

Amendment

1. This Regulation applies to:

Amendment 41

Proposal for a regulation

Article 2 – paragraph 1 – point a (new)

Text proposed by the Commission

Amendment

(a) *the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services, irrespective of whether a payment is required;*

Amendment 42

Proposal for a regulation

Article 2 – paragraph 1 – point b (new)

Text proposed by the Commission

Amendment

(b) *the processing of information related to or processed by the terminal equipment of end-users;*

Amendment 43

Proposal for a regulation

Article 2 – paragraph 1 – point c (new)

Text proposed by the Commission

Amendment

(c) *the placing on the market of software permitting electronic communications including the retrieval and presentation of information on the Internet;*

Amendment 44

Proposal for a regulation

Article 2 – paragraph 1 – point d (new)

Text proposed by the Commission

Amendment

(d) *the provision of publicly available*

directories of users of electronic communications;

Amendment 45

Proposal for a regulation

Article 2 – paragraph 1 – point e (new)

Text proposed by the Commission

Amendment

(e) the sending of direct marketing electronic communications to end-users.

Amendment 46

Proposal for a regulation

Article 3 – paragraph 1 – point a

Text proposed by the Commission

Amendment

(a) the *provision* of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;

(a) the *offering* of electronic communications services, *software, publicly available directories, or direct marketing electronic communications* to end-users in the Union, irrespective of whether a payment of the end-user is required;

Amendment 47

Proposal for a regulation

Article 3 – paragraph 1 – point b

Text proposed by the Commission

Amendment

(b) the *use of such services*;

(b) the *activities referred to in Article 2 that are provided from the territory of the Union*;

Amendment 48

Proposal for a regulation

Article 3 – paragraph 1 – point c

Text proposed by the Commission

(c) the **protection** of information related to the terminal equipment of end-users **located** in the Union.

Amendment

(c) the **processing** of information related to **or processed by** the terminal equipment of end-users **that is** in the Union.

Amendment 49

Proposal for a regulation
Article 3 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. Where the provider of an electronic communications service, **provider of software permitting electronic communications, a person processing information related to or processed by the terminal equipment of users or end-users, a provider of a publicly available directory, or a person using electronic communications services to transmit direct marketing communications** is not established in the Union, it shall designate in writing a representative in the Union.

Amendment 50

Proposal for a regulation
Article 3 – paragraph 4

Text proposed by the Commission

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.

Amendment

4. The representative shall have the power to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, **courts**, and end-users, on all issues related to **the activities referred to in Article 2** for the purposes of ensuring compliance with this Regulation.

Amendment 51

Proposal for a regulation

Article 3 – paragraph 5

Text proposed by the Commission

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***.

Amendment

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.

Amendment 52

Proposal for a regulation

Article 4 – paragraph 1 – point b

Text proposed by the Commission

(b) the ***definitions of ‘electronic communications network’, ‘electronic communications service’, ‘interpersonal communications service’, ‘number-based interpersonal communications service’, ‘number-independent interpersonal communications service’, ‘end-user’ and ‘call’ in points (1), (4), (5), (6), (7), (14) and (21) respectively*** of Article 2 of [Directive establishing the European Electronic Communications Code];

Amendment

(b) the ***definition of ‘call’ in point (21)*** of Article 2 of [Directive establishing the European Electronic Communications Code];

Amendment 53

Proposal for a regulation

Article 4 – paragraph 2

Text proposed by the Commission

2. ***For the purposes of point (b) of paragraph 1, the definition of ‘interpersonal communications service’ shall include services which enable***

Amendment

deleted

interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

Amendment 54

Proposal for a regulation
Article 4 – paragraph 3 – point -a (new)

Text proposed by the Commission

Amendment

(-a) 'electronic communications network' means a transmission system, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit - and packet - switched including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

Amendment 55

Proposal for a regulation
Article 4 – paragraph 3 – point -a a (new)

Text proposed by the Commission

Amendment

(-aa) 'electronic communications service' means a service provided via electronic communications networks, whether for remuneration or not, which encompasses one or more of the following: an 'internet access service' as defined in Article 2(2) or Regulation (EU)

2015/2120; an interpersonal communications service; a service consisting wholly or mainly in the conveyance of the signals, such as a transmission service used for the provision of a machine-to-machine service and for broadcasting, but excludes information conveyed as part of a broadcasting service to the public over an electronic communications network or service except to the extent that the information can be related to the identifiable end-user receiving the information; it also includes services which are not publicly available, but provide access to a publicly available electronic communications network;

Amendment 56

Proposal for a regulation

Article 4 – paragraph 3 – point -a b (new)

Text proposed by the Commission

Amendment

(-ab) 'interpersonal communications service' means a service, whether provided for remuneration or not, that enables direct interpersonal and interactive exchange of information between a finite number of persons whereby the persons initiating or participating in the communication determine the recipient(s);

Amendment 57

Proposal for a regulation

Article 4 – paragraph 3 – point -a c (new)

Text proposed by the Commission

Amendment

(-ac) 'number-based interpersonal communications service' means an interpersonal communications service which connects to the public switched telephone network, either by means of

assigned numbering resources, i.e. number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;

Amendment 58

Proposal for a regulation

Article 4 – paragraph 3 – point -a d (new)

Text proposed by the Commission

Amendment

(-ad) 'number-independent interpersonal communications service' means an interpersonal communications service which does not connect with the public switched telephone network, either by means of assigned numbering resources, i.e. a number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;

Amendment 59

Proposal for a regulation

Article 4 – paragraph 3 – point -a e (new)

Text proposed by the Commission

Amendment

(-ae) 'end-user' means a legal entity or a natural person using or requesting a publicly available electronic communications service;

Amendment 60

Proposal for a regulation

Article 4 – paragraph 3 – point -a f (new)

(-af) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

Amendment 61

Proposal for a regulation

Article 4 – paragraph 3 – point b

Text proposed by the Commission

Amendment

(b) 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;

(b) 'electronic communications content' means the content ***transmitted, distributed or*** exchanged by means of electronic communications services, such as text, voice, videos, images, and sound. ***Where metadata of other electronic communications services or protocols are transmitted, distributed or exchanged by using the respective service, they shall be considered electronic communications content for the respective service;***

Amendment 62

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 data used to trace and identify the source and destination of a communication, ***data on the location of the terminal equipment processed in the context of providing electronic communications services, and the date, time, duration and the type of***

communication;

Amendment 63

Proposal for a regulation

Article 4 – paragraph 3 – point f

Text proposed by the Commission

(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.;

Amendment

(f) ‘direct marketing communications’ means any form of advertising, whether *in* written, *oral or video format, sent, served or presented* to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communications systems with or without human interaction, electronic mail, SMS, *fax machines* etc.;

Amendment 64

Proposal for a regulation

Article 4 – paragraph 3 – point g

Text proposed by the Commission

(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems;

Amendment

(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communications systems, *including calls made using automated calling and communications systems which connect the called person to an individual;*

Amendment 65

Proposal for a regulation

Article 4 – paragraph 3 – point h

Text proposed by the Commission

(h) ‘automated calling and communication systems’ means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and

Amendment

(h) ‘automated calling and communications systems’ means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and

transmitting sounds which are not live speech, ***including calls made using automated calling and communication systems which connect the called person to an individual.***

transmitting sounds which are not live speech.

Amendment 66

Proposal for a regulation Chapter 2 – title

Text proposed by the Commission

PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION ***STORED*** IN THEIR TERMINAL EQUIPMENT

Amendment

PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL PERSONS AND OF INFORMATION ***PROCESSED BY AND RELATED TO*** THEIR TERMINAL EQUIPMENT

Amendment 67

Proposal for a regulation Article 5 – title

Text proposed by the Commission

Confidentiality of electronic communications ***data***

Amendment

Confidentiality of electronic communications

Amendment 68

Proposal for a regulation Article 5 – paragraph 1

Text proposed by the Commission

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.***

Amendment

Electronic communications shall be confidential. Any interference, with electronic communications, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or ***any*** processing of electronic communications, by persons other than the ***end-users***, shall be prohibited.

Amendment 69

Proposal for a regulation Article 5 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1 a. Confidentiality of electronic communications shall also apply to data related to or processed by terminal equipment.

Amendment 70

Proposal for a regulation Article 6 – title

Text proposed by the Commission

Amendment

Permitted processing of electronic communications data

Lawful processing of electronic communications data

Amendment 71

Proposal for a regulation Article 6 – paragraph 1

Text proposed by the Commission

Amendment

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 if it is technically necessary to achieve the transmission of the communication, for the duration necessary for that purpose.***

Amendment 72

Proposal for a regulation Article 6 – paragraph 1 b (new)

1 b. Providers of electronic communications networks and services **or other parties acting on behalf of the provider or the end-user** may process electronic communications data **only if it is technically necessary to maintain or restore the availability, integrity, confidentiality and security of the respective electronic communications network or services, or to detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.**

Amendment 73

Proposal for a regulation

Article 6 – paragraph 2 – introductory part

Text proposed by the Commission

2. Providers of electronic communications services may process electronic communications metadata if:

Amendment

2. Providers of electronic communications services **and networks** may process electronic communications metadata **only** if:

Amendment 74

Proposal for a regulation

Article 6 – paragraph 2 – point a

Text proposed by the Commission

(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120²⁸ for the duration necessary for that purpose; or

Amendment

(a) it is **strictly** necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120²⁸ for the duration **technically** necessary for that purpose; or

²⁸ Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures

²⁸ 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).

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 75

Proposal for a regulation

Article 6 – paragraph 2 – point b

Text proposed by the Commission

(b) it is necessary for billing, **calculating** interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

Amendment

(b) it is **strictly** necessary for billing, **determining** interconnection payments, detecting or stopping fraudulent **use of, or subscription to,** electronic communications services; or

Amendment 76

Proposal for a regulation

Article 6 – paragraph 2 – point c

Text proposed by the Commission

(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**.

Amendment

(c) the 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 **users**, provided that the purpose or purposes concerned could not be fulfilled **without the processing of such metadata**.

Amendment 77

Proposal for a regulation

Article 6 – paragraph 2 a (new)

(2a) *For the purposes of point (c) of paragraph 2, 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, Articles 35 and 36 of Regulation (EU) 2016/679 shall apply.*

Amendment 78

Proposal for a regulation

Article 6 – paragraph 3 – point a

Text proposed by the Commission

(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

Amendment

(a) for the sole purpose of the provision of a specific service *requested by the user*, if the *user* concerned *has* given *his or her* 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*; or

Amendment 79

Proposal for a regulation

Article 6 – paragraph 3 – point b

Text proposed by the Commission

(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

Amendment

(b) if all *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

authority.

consultation of the supervisory authority.

Amendment 80

Proposal for a regulation

Article 6 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. *The provider of the electronic communications service may process electronic communications data solely for the provision of an explicitly requested service, for purely individual usage, only for the duration necessary for that purpose and without the consent of all users only where such requested processing does not adversely affect the fundamental rights and interests of another user or users.*

Amendment 81

Proposal for a regulation

Article 7 – paragraph 1

Text proposed by the Commission

Amendment

1. Without prejudice to **point (b) of Article 6(1)** and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content **or make that data anonymous after receipt of electronic communication content** by the **intended recipient or recipients**. Such data may be recorded or stored by the **end-users** or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

1. Without prejudice to Article **6(1b)** and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content, **when it is no longer necessary for the provision of such service, as requested** by the **user**. Such data may be recorded or stored by the **users** or by a third party entrusted by them to record, store or otherwise process such data. **The user may process the data** in accordance with Regulation (EU) 2016/679.

Amendment 82

Proposal for a regulation

Article 7 – paragraph 2

PE606.011v02-00

54/245

RR\1137482EN.docx

Text proposed by the Commission

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**.

Amendment

2. Without prejudice to Article **6(1b)** 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 **necessary** for the **provision of such service, as requested by the user**.

Amendment 83

**Proposal for a regulation
Article 7 – paragraph 3**

Text proposed by the Commission

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.

Amendment

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), **strictly necessary** 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.

Amendment 84

**Proposal for a regulation
Article 8 – title**

Text proposed by the Commission

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

Amendment

Protection of information **transmitted to,** stored in and related to **processed by and collected from users'** terminal equipment

Amendment 85

**Proposal for a regulation
Article 8 – paragraph 1 – introductory part**

Text proposed by the Commission

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:

Amendment 86

Proposal for a regulation
Article 8 – paragraph 1 – point a

Text proposed by the Commission

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

Amendment 87

Proposal for a regulation
Article 8 – paragraph 1 – point b

Text proposed by the Commission

(b) the **end-user** has given his or her consent; or

Amendment 88

Proposal for a regulation
Article 8 – paragraph 1 – point c

Text proposed by the Commission

(c) it is necessary for providing an information society service requested by the **end-user**; or

Amendment

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 **user** concerned shall be prohibited, except on the following grounds:

Amendment

(a) it is **strictly** necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

Amendment

(b) the **user** has given his or her **specific** consent; or

Amendment

(c) it is **strictly technically** necessary for providing an information society service **specifically** requested by the **user**; or

Amendment 89

Proposal for a regulation

Article 8 – paragraph 1 – point d

Text proposed by the Commission

(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**.

Amendment

(d) if it is **technically** necessary for measuring **the reach of an information society service requested by the user**, provided that such measurement is carried out by the provider, **or on behalf of the provider, or by a web analytics agency acting in the public interest including for scientific purpose; that the data is aggregated and the user is given a possibility to object; and further provided that no personal data is made accessible to any third party and that such measurement does not adversely affect the fundamental rights of the user; Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers; or**

Amendment 90

Proposal for a regulation

Article 8 – paragraph 1 – point d a (new)

Text proposed by the Commission

Amendment

(da) it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:

(i) this does 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 an update is being installed;
and*

*(iii) the user has the possibility to
postpone or turn off the automatic
installation of these updates;*

Amendment 91

Proposal for a regulation

Article 8 – paragraph 1 – point d b (new)

Text proposed by the Commission

Amendment

*(d b) in the context of employment
relationships, it is strictly technically
necessary for the execution of an
employee's task, where:*

*(i) the employer provides and/or is the
user of the terminal equipment;*

*(ii) the employee is the user of the
terminal equipment; and*

*(iii) it is not further used for monitoring
the employee.*

Amendment 92

Proposal for a regulation

Article 8 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

*1a. 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 he or she has not given his or her
consent under Article 8(1)(b) to the
processing of personal information and/or
the use of processing or storage
capabilities of his or her terminal
equipment that is not necessary for the
provision of that service or functionality.*

Amendment 93

Proposal for a regulation

Article 8 – paragraph 2

Text proposed by the Commission

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:

Amendment

2. The **processing** of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:

Amendment 94

Proposal for a regulation

Article 8 – paragraph 2 – subparagraph 1 – point a

Text proposed by the Commission

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or

Amendment

(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 user**; or

Amendment 95

Proposal for a regulation

Article 8 – paragraph 2 – subparagraph 1 – point a a (new)

Text proposed by the Commission

Amendment

(aa) **the user has been informed and has given consent; or**

Amendment 96

Proposal for a regulation

Article 8 – paragraph 2 – subparagraph 1 – point a b (new)

Text proposed by the Commission

Amendment

(ab) **the risks are mitigated.**

Amendment 97

Proposal for a regulation

Article 8 – paragraph 2 – subparagraph 1 – point b

Text proposed by the Commission

Amendment

(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.

deleted

Amendment 98

Proposal for a regulation

Article 8 – paragraph 2 – subparagraph 2

Text proposed by the Commission

Amendment

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.

deleted

Amendment 99

Proposal for a regulation

Article 8 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. For the purpose of points (d) of paragraph 1 and (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; and

(b) the processing shall be limited in time and space to the extent strictly necessary for this purpose; and

(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and

(d) the users shall be given effective possibilities to object that do not affect the functionality of the terminal equipment.

Amendment 100

Proposal for a regulation

Article 8 – paragraph 2 b (new)

Text proposed by the Commission

Amendment

2b. The information referred to in points (aa) and (ab) of paragraph 2 shall be conveyed in a clear and prominent notice setting out, at the least, details of how the information will be collected, the purpose of processing, 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.

Amendment 101

Proposal for a regulation

Article 8 – paragraph 3

Text proposed by the Commission

Amendment

3. The information to be provided pursuant to *point (b) of* paragraph 2 may be provided in combination with

3. The information to be provided pursuant to paragraph 2*b* may be provided in combination with standardized icons in

standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

Amendment 102

Proposal for a regulation Article 9 – paragraph 1

Text proposed by the Commission

1. The definition of and conditions for consent provided for ***under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU*** shall apply.

Amendment

1. The definition of and conditions for consent provided for ***in Regulation (EU) 2016/679/EU*** shall apply.

Amendment 103

Proposal for a regulation Article 9 – paragraph 2

Text proposed by the Commission

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.***

Amendment

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 ***or withdrawn*** by using technical ***specifications for electronic communications services or information society services which allow for specific consent for specific purposes and with regard to specific service providers actively selected by the user in each case, pursuant to paragraph 1. When such technical specifications are used by the user's terminal equipment or the software running on it, they may signal the user's choice based on previous active selections by him or her. These signals shall be binding on, and enforceable against, any other party.***

Amendment 104

Proposal for a regulation Article 9 – paragraph 3

Text proposed by the Commission

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.

Amendment

3. **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), **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 as long as the processing continues.

Amendment 105

Proposal for a regulation Article 9 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3 a. Any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communication, in particular their rights to privacy and the protection of personal data.

Amendment 106

Proposal for a regulation Article 10 – paragraph 1

Text proposed by the Commission

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**

Amendment

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

equipment of an end-user or processing information already stored on that equipment.

Amendment 107

Proposal for a regulation

Article 10 – paragraph 1 – point a (new)

Text proposed by the Commission

Amendment

(a) by default, have privacy protective settings activated to prevent other parties from transmitting to or storing information on the terminal equipment of a user and from processing information already stored on or collected from that equipment, except for the purposes laid down by Article 8(1), points (a) and (c);

Amendment 108

Proposal for a regulation

Article 10 – paragraph 1 – point b (new)

Text proposed by the Commission

Amendment

(b) 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 and offer the option to prevent other parties from processing information transmitted to, already stored on or collected from the terminal equipment for the purposes laid down by Article 8(1) points (a), (c), (d) and (da);

Amendment 109

Proposal for a regulation

Article 10 – paragraph 1 – point c (new)

Text proposed by the Commission

Amendment

(c) offer the user the possibility to express specific consent through the settings after the installation of the software.

Amendment 110

Proposal for a regulation

Article 10 – paragraph 1 – subparagraph 1 (new)

Text proposed by the Commission

Amendment

Before the first use of the software, the software shall inform the user about the privacy settings and the available granular setting options according to the information society service accessed. These settings shall be easily accessible during the use of the software and presented in a manner that gives the user the possibility for making an informed decision.

Amendment 111

Proposal for a regulation

Article 10 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. For the purpose of::

Amendment 112

Proposal for a regulation

Article 10 – paragraph 1 a (new) – point a (new)

Text proposed by the Commission

Amendment

(a) points (a) and (b) of paragraph 1,

Amendment 113

Proposal for a regulation

Article 10 – paragraph 1 a (new) – point b (new)

Text proposed by the Commission

Amendment

(b) giving or withdrawing consent pursuant to Article 9(2) of this Regulation, and

Amendment 114

Proposal for a regulation

Article 10 – paragraph 1 a (new) – point c (new)

Text proposed by the Commission

Amendment

(c) objecting to the processing of personal data pursuant to Article 21(5) of Regulation (EU) 2017/679,

Amendment 115

Proposal for a regulation

Article 10 – paragraph 1 a (new) – subparagraph 1 (new)

Text proposed by the Commission

Amendment

the settings shall lead to a signal based on technical specifications which is sent to the other parties to inform them about the user's intentions with regard to consent or objection. This signal shall be legally valid and be binding on, and enforceable against, any other party.

Amendment 116

Proposal for a regulation

Article 10 – paragraph 1 b (new)

Text proposed by the Commission

Amendment

1b. In accordance with Article 9 paragraph 2, such software shall ensure

that a specific information society service may allow the user to express specific consent. A specific consent given by a user pursuant to point (b) of Article 8(1) shall prevail over the existing privacy settings for that particular information society service. Without prejudice to paragraph 1, where a specified technology has been authorised by the data protection board for the purposes of point (b) of Article 8(1), consent may be expressed or withdrawn at any time both from within the terminal equipment and by using procedures provided by the specific information society service.

Amendment 117

Proposal for a regulation Article 10 – paragraph 2

Text proposed by the Commission

Amendment

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.*

deleted

Amendment 118

Proposal for a regulation Article 10 – paragraph 3

Text proposed by the Commission

Amendment

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**.

3. In the case of software which has already been installed on *[xx.xx.xxxx]*, the requirements under paragraphs 1, ***1a*** and ***1b*** shall be complied with at the time of the first update of the software, but no later than ***six months after [the date of entry into force of this Regulation]***.

Amendment 119

Proposal for a regulation Article 11

Text proposed by the Commission

Amendment

Article 11

deleted

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 official authority for such interests.

2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

Amendment 120

Proposal for a regulation Article 11 a (new)

Text proposed by the Commission

Amendment

Article 11a

Restrictions on the rights of the user

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 principles relating to processing of electronic communications data provided for in Articles 6, 7 and 8 of this Regulation in so far as its provisions correspond to the rights and obligations provided for in Regulation (EU) 2016/679, when such a restriction fully 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 (d) of Regulation (EU) 2016/679.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, pursuant to Article 23(2) of Regulation (EU) 2016/679.

Amendment 121

Proposal for a regulation Article 11 b (new)

Text proposed by the Commission

Amendment

Article 11b

Restrictions on confidentiality of communications

1. Union or Member State law may restrict by way of a legislative measure the scope of the rights provided for in Article 5 where such a restriction fully 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 following general public interests:

- (a) national security;*
- (b) defence;*

- (c) *public security;*
- (d) *the prevention, investigation, detection or prosecution of serious criminal offences, unauthorised use of electronic communication systems or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*

2. *In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, pursuant to Article 23(2) of Regulation (EU) 2016/679.*

Amendment 122

Proposal for a regulation Article 11 c (new)

Text proposed by the Commission

Amendment

Article 11 c

Documentation and reporting of restrictions

1. *Providers of electronic communications services shall keep documentation about requests made by competent authorities to access communications content or metadata pursuant to Article 11b(2). This documentation shall include for each request:*

- (a) *the in-house staff member who handled the request;*
- (b) *the identity of the body making the request;*
- (c) *the purpose for which the information was sought;*
- (d) *the date and time of the request;*
- (e) *the legal basis and authority for the request, including the identity and status or function of the official submitting the request;*

(f) the judicial authorisation of the request;

(g) the number of users to whose data the request related;

(h) the data provided to the requesting authority; and

(i) the period covered by the data.

The documentation shall be made available to the competent supervisory authority upon request.

2. Providers of electronic communications services shall publish once per year a report with statistical information about data access requests by law enforcement authorities pursuant to Articles 11a and 11b. The report shall include, at least:

(a) the number of requests;

(b) the categories of purposes for the request;

(c) the categories of data requested;

(d) the legal basis and authority for the request;

(e) the number of users to whose data the request related;

(f) the period covered by the data;

(g) the number of negative and positive responses to those requests.

3. Member States' competent authorities shall publish once per year a report with statistical information per month about data access requests pursuant to Articles 11a and 11b, including requests that were not authorised by a judge, including, but not limited to, the following points:

(a) the number of requests;

(b) the categories of purposes for the request;

(c) the categories of data requested;

(d) the legal basis and authority for the

request;

(e) the number of users to whose data the request related;

(f) the period covered by the data;

(g) the number of negative and positive responses to those requests.

The reports shall also contain statistical information per month about any other restrictions pursuant to Articles 11a and 11b.

Amendment 123

Proposal for a regulation Article 13 – paragraph 1

Text proposed by the Commission

1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an *end-user* for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.

Amendment

1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of *a user* for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.

Amendment 124

Proposal for a regulation Article 13 – paragraph 2

Text proposed by the Commission

2. *Member States shall establish more specific provisions* with regard to the establishment of procedures and the circumstances where providers of publicly

Amendment

2. *The Commission shall be empowered to adopt implementing measures in accordance with Article 26(1)* with regard to the establishment of

available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where *end-users* request the tracing of malicious or nuisance calls.

procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where *users* request the tracing of malicious or nuisance calls.

Amendment 125

Proposal for a regulation

Article 14 – paragraph 1 – introductory part

Text proposed by the Commission

Providers of publicly available number-based interpersonal communications services *shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also* provide the called end-user with the following possibilities, free of charge:

Amendment

Providers of publicly available number-based interpersonal communications services provide the called end-user with the following possibilities, free of charge:

Amendment 126

Proposal for a regulation

Article 14 – paragraph 1 – point a

Text proposed by the Commission

(a) to block incoming calls from specific numbers or from anonymous sources;

Amendment

(a) to block incoming calls from specific numbers, *or numbers having a specific code or prefix identifying the fact that the call is a marketing call referred to in Article 16(3)(b)*, or from anonymous sources;

Amendment 127

Proposal for a regulation

Article 14 – paragraph 1 – point b

Text proposed by the Commission

(b) to stop automatic call forwarding

Amendment

(b) to stop automatic call forwarding

by a third party to the *end-user's* terminal equipment.

by a third party to the *user's* terminal equipment.

Amendment 128

Proposal for a regulation Article 15 – paragraph 1

Text proposed by the Commission

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.*

Amendment

1. *Without prejudice to Articles 12 to 22 of Regulation (EU) 2016/679, the electronic communication services providers shall obtain the consent of users to include their personal data in the publicly available directory and, consequently, shall obtain consent from these users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory. Electronic communication service providers shall give users the means to verify, correct, update, supplement and delete such data. When electronic communication service providers obtain consent of users, they shall make users' data available for public directory providers in an immediate, non-discriminatory and fair manner.*

Amendment 129

Proposal for a regulation Article 15 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. The providers of a publicly available directory shall inform *users* whose personal data are in the directory of the available search functions of the directory and *provide the users the option to disable* such search functions related to their own data.

Amendment 130

Proposal for a regulation Article 15 – paragraph 3

Text proposed by the Commission

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.

Amendment

3. The *electronic communication service* providers shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. *Electronic communication service* providers shall give such end-users that are legal persons the means to verify, correct and delete such data. *For the purposes of this Article, natural persons acting in a professional capacity, such as independent professionals, operators of small businesses or freelancers, shall be equated with legal persons, as regards their data related to their professional capacity.*

Amendment 131

Proposal for a regulation Article 15 – paragraph 4

Text proposed by the Commission

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

4. *Without prejudice to Article 12(5) of Regulation (EU) 2016/679, the information to the users and the possibility not to be included in a publicly available directory, or to verify, correct, update, supplement and delete any data related to them shall be provided free of charge and in an easily accessible manner by the electronic communication services providers.*

Amendment 132

Proposal for a regulation Article 15 – paragraph 4 a (new)

4 a. *Where the personal data of the users of number-based interpersonal communications services have been included in a publicly available directory before this Regulation enters into force, the personal data of such users may remain included in a publicly available directory, including versions with search functions, unless the users have expressed their objection against their data being included in the directory or against available search functions related to their data.*

Amendment 133

Proposal for a regulation Article 16 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. *The use by* natural or legal persons *of electronic communications services, including automated calling, communications systems, 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 or* sending direct marketing communications *to users, shall be allowed only in respect of users who* have given their *prior* consent.

Amendment 134

Proposal for a regulation Article 16 – paragraph 2

Text proposed by the Commission

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

Amendment

2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a

service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own *similar* products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.

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 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 ***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 135

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

Text proposed by the Commission

Amendment

3 a. The masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited communications for direct marketing purposes is prohibited.

Amendment 136

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.

4. Notwithstanding paragraph 1, the placing of direct marketing voice-to-voice calls to ***users*** shall only be allowed in respect of ***users*** who have not expressed their objection to receiving those communications. ***Member States shall provide that users can object to receiving the direct marketing voice-to-voice calls via a Do Not Call Register, thereby also ensuring that the user needs to opt-out only once.***

Amendment 137

Proposal for a regulation Article 16 – paragraph 6

Text proposed by the Commission

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.

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 **and free of charge**, to receiving further marketing communications.

Amendment 138

Proposal for a regulation Article 16 – paragraph 7

Text proposed by the Commission

7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.

Amendment

7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(1) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.

Amendment 139

Proposal for a regulation Article 17 – paragraph 1

Text proposed by the Commission

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

Amendment

Providers of electronic communications services shall comply with the security obligations as prescribed Regulation (EU) 2016/679 and [European Electronic Communications Code]. As regards the security of networks and services and

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.*

related security obligations, the obligations of Article 40 of the [European Electronic Communications Code] shall apply mutatis mutandis to all services in the scope of this Regulation. This Article shall be without prejudice to the obligations provided for in Articles 32 to 34 of Regulation (EU) 2016/679 and the obligations provided for in Directive (EU) 2016/1148.

Amendment 140

Proposal for a regulation Article 17 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

(1a) Providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the confidentiality and integrity of the communication in transmission or stored are also guaranteed by technical measures according to the state of the art, such as cryptographic methods including end-to-end encryption of the electronic communications data. When encryption of electronic communications data is used, decryption by anybody else than the user shall be prohibited. Notwithstanding Articles 11a and 11b of this Regulation, member States shall not impose any obligations on electronic communications service providers or software manufacturers that would result in the weakening of the confidentiality and integrity of their networks and services or the terminal equipment, including the encryption methods used.

Amendment 141

Proposal for a regulation Article 17 – paragraph 1 b (new)

Text proposed by the Commission

Amendment

(1b) Providers of electronic communications services, providers of information society services, and manufacturers of software permitting the retrieval and presentation of information on the internet shall not use any means, no matter if technical, operational, or by terms of use or by contracts, that could prevent users and subscribers from applying the best available techniques against intrusions and interceptions and to secure their networks, terminal equipment and electronic communications. Notwithstanding Articles 11a and 11b of this Regulation, breaking, decrypting, restricting or circumventing such measure taken by users or subscribers shall be prohibited.

Amendment 142

Proposal for a regulation Article 17 – paragraph 1 c (new)

Text proposed by the Commission

Amendment

(1c) In the case of a particular risk that may compromise the security of networks, electronic communications services, information society services or software, the relevant provider or manufacturer shall inform all subscribers of such a risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform subscribers of any possible remedies. It shall also inform the relevant manufacturer and service provider.

Amendment 143

Proposal for a regulation Article 18 – paragraph 1

Text proposed by the Commission

1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.

Amendment

1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*. ***Where Regulation (EU) 2016/679 refers to data subjects, the tasks and powers of the supervisory authorities shall be exercised with regard to end-users under this Regulation. Where Regulation (EU) 2016/679 refers to data controllers, the tasks and powers of the supervisory authorities shall be exercised with regard to providers of electronic communications services and information society services, and manufacturers of software under this Regulation.***

Amendment 144

Proposal for a regulation

Article 19 – paragraph 1 – point b a (new)

Text proposed by the Commission

Amendment

(ba) draw up guidelines for supervisory authorities concerning the application of Article 9(1) and the particularities of expression of consent by legal entities;

Amendment 145

Proposal for a regulation

Article 19 – paragraph 1 – point b b (new)

Text proposed by the Commission

Amendment

(bb) issue guidelines to determine which technical specifications and signalling methods fulfil the conditions and objectives pursuant to Article 10(1a);

Amendment 146

Proposal for a regulation

Article 19 – paragraph 1 – point b c (new)

Text proposed by the Commission

Amendment

(bc) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph for the purpose of further specifying the criteria and requirements for types of services that may be requested for purely individual or work-related usage as referred to in Article 6(3a):

Amendment 147

Proposal for a regulation

Article 19 – paragraph 1 – point b d (new)

Text proposed by the Commission

Amendment

(bd) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph for the purpose of further specifying the criteria and requirements for:

(i) measuring the reach of an information society service referred to in Article 8(1) point (d);

(ii) security updates referred to in Article 8(1) point (da);

(iii) the interference in the context of employment relationships referred to in Article 8(1) point (db);

(iv) the processing of information

emitted by the terminal equipment referred to in Article 8(2) ();

(v) technical specifications and signalling methods that fulfil the conditions for consent and objection pursuant to Article 8(2a);

(vi) software settings referred to in Article 10(1a) and (1b); and

(vii) technical measures to ensure confidentiality and integrity of the communication pursuant to Article 17(1a), (1b) and (1c).

Amendment 148

Proposal for a regulation Article 21 – paragraph 1

Text proposed by the Commission

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.

Amendment

1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services **and, where applicable, every body, organisation or association**, shall have the same remedies provided for in Articles 77, 78, **79 and 80** of Regulation (EU) 2016/679.

Amendment 149

Proposal for a regulation Article 21 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1 a. Without prejudice to any other administrative or non-judicial remedy, every end-user of electronic communications services shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him or her. End-users shall also have such a right where the supervisory authority does

not handle a complaint or does not inform the end- user within three months on the progress or outcome of the complaint lodged. Proceedings against a supervisory authority shall be brought before the court of the Member State where the supervisory authority is established.

Amendment 150

Proposal for a regulation

Article 21 – paragraph 1 b (new)

Text proposed by the Commission

Amendment

1 b. Every end-user of the communications services shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed. Those proceedings against a provider of electronic communication service, the provider of a publicly available directory, software provider enabling electronic communication or persons sending direct marketing commercial communications or collecting information related to or stored in the end-users terminal equipment shall be brought before the courts of the Member State where they have an establishment. Alternatively, such proceedings shall be brought before the court of the Member State of the habitual residence of the end-user.

Amendment 151

Proposal for a regulation

Article 23 – paragraph 1

Text proposed by the Commission

Amendment

1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this

1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this

Regulation.

Regulation, *mutatis mutandis*.

Amendment 152

Proposal for a regulation

Article 23 – paragraph 2 – point a

Text proposed by the Commission

Amendment

(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;

deleted

Amendment 153

Proposal for a regulation

Article 23 – paragraph 2 – point a a (new)

Text proposed by the Commission

Amendment

(a a) the obligations of the providers of electronic communications services pursuant to Article 11c;

Amendment 154

Proposal for a regulation

Article 23 – paragraph 2 – point b

Text proposed by the Commission

Amendment

(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;

deleted

Amendment 155

Proposal for a regulation

Article 23 – paragraph 2 – point b a (new)

Text proposed by the Commission

Amendment

(b a) the obligations of the providers of publicly available number-based

Amendment 156

Proposal for a regulation

Article 23 – paragraph 3

Text proposed by the Commission

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.

Amendment

3. Infringements of the *following provisions of this Regulation* shall, in accordance with paragraph 1, 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:

Amendment 157

Proposal for a regulation

Article 23 – paragraph 3 – point a (new)

Text proposed by the Commission

Amendment

(a) *the principle of confidentiality of communications pursuant to Article 5;*

Amendment 158

Proposal for a regulation

Article 23 – paragraph 3 – point b (new)

Text proposed by the Commission

Amendment

(b) *the permitted processing of electronic communications data, pursuant to Article 6;*

Amendment 159

Proposal for a regulation

Article 23 – paragraph 3 – point c (new)

Text proposed by the Commission

Amendment

(c) the time limits for erasure and the confidentiality obligations pursuant to Article 7;

Amendment 160

Proposal for a regulation

Article 23 – paragraph 3 – point d (new)

Text proposed by the Commission

Amendment

(d) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;

Amendment 161

Proposal for a regulation

Article 23 – paragraph 3 – point e (new)

Text proposed by the Commission

Amendment

(e) the requirements for consent pursuant to Article 9;

Amendment 162

Proposal for a regulation

Article 23 – paragraph 3 – point f (new)

Text proposed by the Commission

Amendment

(f) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;

Amendment 163

Proposal for a regulation

Article 23 – paragraph 3 – point g (new)

Text proposed by the Commission

Amendment

(g) the obligations of the providers of electronic communications services, of the providers of information society services, or of the manufacturers of software permitting the retrieval and presentation of information on the internet pursuant to Article 17.

Amendment 164

Proposal for a regulation

Article 23 – paragraph 4

Text proposed by the Commission

Amendment

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

4. In the event that the same act or omission by the same person results in non-compliance with both Regulation (EU) 2016/679 and this Regulation, then the maximum administrative fine shall be no more than the maximum administrative fine applicable under this Regulation for that type of infringement.

Amendment 165

Proposal for a regulation

Article 26 – paragraph 1

Text proposed by the Commission

Amendment

1. The Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code]. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011²⁹.

1. For the purpose of Articles 13(2) and 16(7), the Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code]. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011²⁹.

²⁹ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13–18).

²⁹ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13–18).

Amendment 166

Proposal for a regulation Article 27 – paragraph 1

Text proposed by the Commission

1. Directive 2002/58/EC *is* repealed with effect from **25 May 2018**.

Amendment

1. Directive 2002/58/EC *and Commission Regulation 611/2013 are* repealed with effect from *[XXX]*.

Amendment 167

Proposal for a regulation Article 28 – paragraph 1

Text proposed by the Commission

By **1 January 2018** at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.

Amendment

By *[the date of entry into force of this Regulation]* at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.

Amendment 168

Proposal for a regulation Article 29 – paragraph 2 – subparagraph 1

Text proposed by the Commission

It shall apply from **25 May 2018**.

Amendment

It shall apply from *[one year the date of entry into force of this Regulation]*.

EXPLANATORY STATEMENT

Introduction

The Charter of Fundamental Rights of the European Union, legally binding since the entry into force of the Treaty of Lisbon, establishes in its Article 7 the right of private life:

“Everyone has the right to respect for his or her private and family life, home and communications”.

Article 8 establishes the right to the protection of personal data in the following terms

- “1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.”

Article 16 of the Treaty on the Functioning of the European Union provides the legal basis for the adoption of Union legal instruments relating to the protection of personal data.

On 10 January 2017 the Commission has presented a proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC) (ePrivacy Regulation).

The ePrivacy Directive (2002/58/EC) has set forth rules guaranteeing the protection of privacy in the electronic communications sector. It aimed to ensure that the protection of confidentiality of communications, in line with the fundamental right to the respect of private and family life enshrined in Article 7 of the EU Charter of Fundamental Rights, is guaranteed. The rules it established complemented and particularised those of Directive 95/46/EC (i.e. the Data Protection Directive) which had set out the general legal framework for the protection of personal data in the Union.

Since then, the Union has engaged in a profound review of the Union data protection legal framework in order to create a modern, robust and overall framework ensuring a high level of protection of individuals granting them the control over their personal data and at the same time cutting red tape for entities processing personal data. Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) establishes the Union legal framework for data protection. It will be applicable as of 25 May 2018.

The ePrivacy regulation proposal

The present ePrivacy proposal seeks to achieve the modernisation of the Union data protection legal framework commenced by the GDPR. It repeals the current ePrivacy Directive 2002/58/EC in order to align its rules to those of the GDPR and to establish a legal framework, which takes account of the important technological and economic developments in the electronic communication sector since the adoption of the ePrivacy Directive in 2002. Today new services of interpersonal communications (Over-The-Top (OTT) providers etc.), as well as machine-to-machine communications and “Internet of Things” (IoT) coexist in parallel with traditional communication services presenting new challenges and risks concerning the privacy and the protection of personal data of individuals. These new services were not covered in the scope of the Directive 2002/58, resulting therefore in a gap of protection. The new proposal takes into account the experience gathered over the years regarding cookies and other tools enabling tracking of individuals that seriously affect the private life and confidentiality of communications. Finally, it takes stock of the recent case law of the Court of Justice.

The Commission states that this proposal is a key element of the completion of the Digital Single Market Strategy, as it would increase trust and security of digital services, which is a precondition to the achievement of the Digital Single Market Strategy.

The ePrivacy proposal, *lex specialis* to the GDPR

Similarly, to the articulation between the ePrivacy Directive 2002/58/EC and the Directive 95/46/EC, the proposed ePrivacy Regulation particularises and complements the General Data Protection Regulation 2016/679. The e-Privacy proposal is a *lex specialis* to the GDPR as regards electronic communications data that are personal data.

The e-privacy also seeks to ensure and protect the right to the confidentiality of communications, enshrined in Article 7 of the Charter and Article 8 of the European Convention of Human Rights, which have been the object of an extensive and detailed case law by both the ECJ and the ECtHR. The ECJ has confirmed the importance of the confidentiality of communications in its cases “Digital rights Ireland” and “Tele 2 and Watson”.

ePrivacy Regulation should ensure a high level of protection

The rules of the ePrivacy Regulation should not lower the level of protection afforded by the General Data Protection Regulation.

However, the opinions of data protection authorities (EDPS, WP29), as well as numerous scholars and stakeholders consulted by your rapporteur for the preparation of this report, allow to conclude that several provisions of the Commission’s proposal would actually lower the level of protection currently afforded by Union law.

Communications data (both content and metadata) are extremely sensitive as they reveal sensitive aspects of the private life of individuals (sexual orientation, philosophical or political beliefs, freedom of expression and information, financial situation, health condition), therefore they deserve a high level of protection. Your rapporteur considers that for this reason, the Commission’s proposal, in order not to lower the high level of protection ensured

by the GDPR, needs to be amended in order to ensure that it will deliver a high level of protection corresponding at least to that offered by the GDPR.

The scope of the ePrivacy proposal

The ePrivacy proposal expands its scope to cover the new forms of electronic communications and ensure the same level of protection of individuals regardless of the communication service used (OTTs, Internet of Things and machine-to-machine interaction).

Your rapporteur supports the Commission's proposal of extending the scope to cover these new channels and forms of electronic communications. She deems it necessary to clarify that the proposal should apply to the use of electronic communications services and to information related to and processed by the terminal equipment of end-users, as well as to the software permitting end-users' electronic communications, but also sending direct marketing commercial communications or collecting (other) information related to or stored in end users terminal equipment by other parties.

The e-Privacy should also be a stand alone instrument and contain all the relevant provisions avoiding dependence from the Electronic Communications Code (ECC). The definitions of the ECC are included in the proposal, when necessary adapted in order to take account of the subject matter of the proposal; (i.e. the protection of the rights of confidentiality of communications and of data protection).

Likewise a definition of "user", inspired by the current e-Privacy Directive is included in order to protect the rights of the individual actually using a publicly available electronic communications service without necessarily being a subscriber. Your Rapporteur also wishes to keep the definition of end-user, as proposed by the Commission, in order to clarify the situations where also legal entities are covered by the protection of this Regulation.

The definition of electronic communications metadata is also amended in order to clarify this concept.

Confidentiality of communications (Articles 5- 7)

The proposal follows the current ePrivacy Directive, and stresses the confidentiality of electronic communications. It recognises a long standing and fundamental right of individuals, enshrined in the ECHR and the EU Charter. The amendments proposed seek to take account of technological development since the adoption of the ePrivacy Directive. Today electronic communications remain stored with service providers even after receipt. Hence, it is proposed to make it clear that the confidentiality of communications is also ensured with regard communications stored or processed by the terminal equipment or other equipment (e.g. cloud storage) as well as communications in the IoT environment (machine-to-machine), when it is related to a user.

Since the right to confidentiality of communications is a fundamental right recognised by the Charter, legally binding upon the EU and the Member States, any interference with it, must be limited to what is strictly necessary and proportionate in a democratic society. Your rapporteur proposes several amendments to Article 6, providing for the conditions allowing the lawful interference with the right of confidentiality of communication in order to process

electronic communications data in specific circumstances and under specific conditions.

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

The rapporteur welcomes the objective of the proposal of the Commission to protect the information stored in the user's terminal equipment from accessing it or installing or placing software or information without the consent of the user (Article 8).

However, you rapporteur is of the view that the regime proposed by the Commission does not fully ensure a high level of protection, on the contrary it would even lower that afforded by the GDPR. Since information processed or stored in terminal equipment or processed during connection to another device or network equipment (eg free Wi-Fi, hotspots) may reveal very sensitive details of an individual, the processing of this information would be subject to very strict conditions under the GDPR. Therefore, the amendments tabled should ensure legal consistency with the GDPR. In this regard, the conditions allowing access to user's terminal equipment or to information emitted by it are better framed (Article 8(1)). The so-called "tracking walls" are forbidden (Article 8(1) 1b)), and the conditions for user's consent is brought in line with the GDPR. Moreover, the use of analytics tools for web audience measuring is clearly defined to take account of the actual techniques used and to ensure that this information is exclusively used for this specific purpose.

Article 8(2) is also amended to ensure that tracking of the location of the terminal equipment that happens for instance on the basis of Wi-Fi or Bluetooth signals is brought into line with the GDPR.

Article 10 of the proposal refers to options for privacy settings of tools and software used to enable users to prevent other parties from storing information on terminal equipment, or processing information stored on the equipment (Do-Not-Track mechanisms -DNTs-). The rapporteur shares the objective of the proposal but she considers that, in order to reflect the essential core principles of Union data protection law (privacy by design and by default), it must be amended. Indeed, these basic principles are not efficiently integrated in the ePrivacy proposal of the Commission. Therefore it is proposed first, that DNTs are technologically neutral to cover different kinds of technical equipment and software and, second, that DNTs, by default must configure their settings in a manner that prevents other parties from storing information on the terminal equipment or processing information stored on the equipment without the consent of the user, at the same time users should be granted the possibility to change or confirm the default privacy settings options at any moment upon installation. The settings should allow for granulation of consent by the user, taking into account the functionality of cookies and tracking techniques and DNTs should send signals to the other parties informing them of the user's privacy settings. Compliance with these settings should be legally binding and enforceable against all other parties.

Presentation of calls, directories of subscribers and direct marketing (Articles 12-16)

Your rapporteur broadly supports the provisions of the proposal relating to the presentation of calls, incoming call blocking and publicly available directories.

Regarding unsolicited communications for direct marketing purposes (Article 16), the amendments tabled clarify the scope of the provision to cover the different kinds of means or

techniques used for direct marketing; the use of direct marketing should be allowed only with regard to natural or legal persons who have given their prior consent. Moreover, withdrawal of consent or objecting to direct marketing communications should be possible at any time and free of charge for the user. Article 16(3) frames conditions for placing unsolicited direct marketing calls and strengthens the safeguards for individuals. Unsolicited communications shall be clearly recognisable as such and shall indicate the identity of the person or entity transmitting the communication or on behalf of whom the communication is transmitted and provide the necessary information for recipient to exercise their right to oppose to receiving further marketing messages.

Supervisory authorities

Your rapporteur fully agrees with the Commission's proposal stating that the independent supervisory authorities for ensuring compliance with the ePrivacy Regulation be the data protection authorities in charge of the supervision of the GDPR. Since the ePrivacy Regulation complements and particularises the GDPR, entrusting to the same independent authorities the tasks of supervision and enforcing compliance of this Regulation will ensure consistency. Cooperation with national regulatory authorities established pursuant to the Electronic Communications Code (ECC) for monitoring the compliance with the rules set forth in this instrument within their respective task shall be ensured.

The regime of fines and sanctions is also amended to cover infringements of the e-Privacy Regulation in line with the GDPR.

Conclusion

The rapporteur supports the objective of this proposal of establishing a modern comprehensive and technologically neutral framework for electronic communications in the Union, which ensures a high level of protection of individuals with regard to their fundamental rights of private life and data protection. Yet she considers that some aspects must be strengthened in order to guarantee a high level of protection as afforded by Regulation (EU) 2016/679, the Charter of Fundamental Rights and the ECHR. The achievement of a Digital Single Market builds on a reliable legal framework for electronic communications that will increase trust of individuals on digital economy and will also allow businesses to pursue their activities in full respect of fundamental rights.

In the preparation of this report, your rapporteur has conducted extensive and thorough discussions with the following stakeholders representing various interests.

The rapporteur expects her proposals to form a good basis for swift agreement in the European Parliament and negotiations with the Council in order to ensure that the legal framework is in place by 25 May 2018.

**ANNEX: LIST OF ENTITIES
FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT**

Access Now
American Chamber of Commerce
App Developers Alliance
Apple
Article 29 Working Party
Association of Commercial Television in EU
AT&T

Bitkom
Bla Bla Car
Booking.com
Bouygues Europe
Business Europe

CENTR
Cisco
CNIL, the French Data Protection Authority
Computer and Communications Industry Association (ccia)
Confederation of Industry of Czech Republic
Cullen International

Deutsche Telekom
Digital Europe
Dropbox
Dutch Data Protection Authority

EBU
EGTA
EMMA
ENPA
Etno
EU Tech Alliance
Eurocommerce
European Association of Communications Agencies
European Commission
European Consumer Organisation (BEUC)
European Data Protection Supervisor
European Digital Media Association
European Digital Rights (EDRI)
European eCommerce and Omni-channel Trade Association
European Publishers Council
EYE/O

Facebook
Federation of European Direct and Interactive Marketing

Federation of German Consumer Organisations (VZBV)
Finnish Federation of Commerce

German Advertising Federation
Google

IAB
Industry Coalition for Data Protection
Interactive Software Federation of Europe

King
KPN

La quadrature du net

Microfost
Mozilla

Nielsen

Open Xchange

Pagefair
Permanent Representation of Germany
Permanent Representation of Spain
Permanent Representation of Sweden
Privasee

Qualcomm

Rakuten

Samsung
Seznam
Siinda
Spotify
Swedish Trade Federation
Symantec
Syndika

Telefonica
The software Alliance (BSA)

Verizon
Video Gaming Industry
Vodafone

World Federation of Advertisers

04.10.2017

OPINION OF THE COMMITTEE ON INDUSTRY, RESEARCH AND ENERGY

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: Kaja Kallas

SHORT JUSTIFICATION

The European Commission proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC aims at the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector but also guarantees the free movement of electronic communications data, equipment and services in the Union.

The Rapporteur is generally supportive of the Commission's proposal, in particular the need to adapt it to technological innovation and new means of communication, in order for this legislation to meet its objectives and be fit for purpose.

Free flow of data and protection of personal data in the Union

The rapporteur welcomes the change of legal instrument from a Directive to a Regulation. The implementation of the former Directive has shown diverging implementations and different interpretations of the law. The rapporteur therefore believes that a Regulation could be a better tool to ensure the protection of personal data in communications of natural and legal persons and safeguards the free flow of data across the Union. The rapporteur however believes that there is a need for the European data protection board to play a more important role in ensuring consistency in the enforcement of this Regulation, in particular by issuing guidance and opinions, building on the consistency mechanism set out in Regulation (EU) 2016/679. In addition, the rapporteur welcomes the task given to data protection authorities to enforce this regulation while stressing that data protection should become more and more a horizontal matter and all authorities should cooperate to this effect, providing technical assistance where necessary to break silos.

Scope

The rapporteur supports the extension of the scope of this Regulation to over-the-top services in light of the increasing role of such services in enabling communications, and the link of the proposed regulation with the definitions set out in the Proposed Directive establishing the European electronic communications Code. The rapporteur stresses however the need to ensure consistency and coherence between the definition in the Code and the e-privacy regulation to avoid loopholes but also risks of inapplicability of some provisions to certain types of services.

Technology neutrality

The rapporteur welcomes the intention and efforts of the Commission in trying to address the complex issue of “consent fatigue” and the need to find more user friendly ways to inform end-users and gives them choices with regard to their privacy. The rapporteur however considers that the proposal of the Commission is too focused on websites while the trend is moving more and more towards apps, IoT platforms and so on. The solutions proposed are too narrowly focused on browsers which risks preventing the regulation to stand the test of time. In addition, the proposal makes a strict distinction between first party cookies and third party cookies. The rapporteur believes that this distinction is not future proof in light of the fast-moving innovation of the digital sector, where a first party cookie can move on to gathering data as a third party cookie, or where other tracking techniques are no longer based on first or third party cookies. The impact on privacy of a cookie should rather be based on its purpose, for instance if the purpose of gathering information is for behaviour based marketing and used cross device, on the types of information it collects, and how the information gathered is shared. The rapporteur therefore does not believe that the strict distinction between first party and third party cookies is the most effective. The user should be better informed, have access to more transparency on the way cookies function, and be able to opt in.

Notice and standardised icons

The rapporteur does not support the possibility of collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment, if there is a sign informing users that this is a tracking area. Such provision creates a risk of fears and anxiety among end-users without providing them a concrete and practical option to opt out of being tracked.

AMENDMENTS

The Committee on Industry, Research and Energy 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 7

Text proposed by the Commission

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

Amendment 2

Proposal for a regulation Recital 9 a (new)

Text proposed by the Commission

Amendment

(7) The **European Data Protection Board** should, **where necessary, issue guidance and opinions** within the limits of this Regulation, to further clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. **Such guidance and opinions should take into account the dual objective of this Regulation and should** therefore maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.

Amendment

(9a) For the purpose of this Regulation, where the provider of an electronic communications service is not established in the Union, it should designate a representative in the Union. The representative should be designated in writing. The representative may be the same as the one designated under Article 27 of Regulation (EU) 2016/679^{1a}.

^{1a} **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) (OJ L 119, 4.5.2016, p. 1).**

Amendment 3

Proposal for a regulation
Recital 11

Text proposed by the Commission

(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 Code²⁴]. 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.***

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

(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 Code²⁴]. 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.

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 4

Proposal for a regulation

Recital 12

Text proposed by the Commission

(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.

Amendment

(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. ***It should not however apply to machine to machine communications that have no impact on either privacy or the confidentiality of communications, such as transmission between network elements (servers, switches).*** Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.

Amendment 5

Proposal for a regulation

Recital 12 a (new)

Text proposed by the Commission

Amendment

(12a) Intelligent Transport Systems need additional protection in this Regulation regarding communications data as connected cars generate, transmit and store users' personal data. Personal

privacy of consumers in connected vehicles needs to be guaranteed, as third parties access and use driver and driving data.

Amendment 6

Proposal for a regulation

Recital 13

Text proposed by the Commission

(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.

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, *airports, hotels, universities*, hospitals *or other such internet access points*. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation. *The mere act of requiring a password should not be considered as providing access to a closed group of end-users if the access is provided to an undefined group of end-users.*

Amendment 7

Proposal for a regulation Recital 14

Text proposed by the Commission

(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.

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 processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. ***It should also include location data, such as for example, the actual or inferred location of the terminal equipment, the location of the terminal equipment from or to which a phone call or an internet connection has been made, or the Wi-Fi hotspot that a device is connected to, as well as data necessary to identify end-users' terminal equipment.*** Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.

Amendment 8

Proposal for a regulation Recital 15 a (new)

Text proposed by the Commission

Amendment

(15 a) Anonymity of data should be considered as an extra layer of protection and confidentiality. Relative provisions should be put in place to anonymise data by default, when possible. Such procedures should be accompanied by a series of tests serving as a proof of anonymity.

Amendment 9

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, ***confidentiality, integrity, availability, authenticity*** and continuity of the electronic communications services ***and networks***, 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.

Amendment 10

Proposal for a regulation Recital 17

Text proposed by the Commission

(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 heat maps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing

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 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 heat maps; 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 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.

structure. Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679. ***The further processing of metadata for purposes other than those for which they were initially collected should only be allowed in cases where the processing is compatible with the initial purpose for which consent was obtained and is subject to specific safeguards, especially pseudonymisation as set forth in point (4) of Article 6 of Regulation (EU) 2016/679.***

Amendment 11

Proposal for a regulation Recital 19

Text proposed by the Commission

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined

Amendment

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined

material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.

material. *For services that are provided to users engaged in purely personal or household activities, for example text or voice service, organisation of the mailbox or SPAM filter service, the consent of the end-user requesting the service should be sufficient.* Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679. *Where communications data are stored by a third party, this third party should ensure that any information whose processing is not necessary to provide the service requested by the end-user is protected with state of the art security measures applied from end to end, including cryptographic methods such as encryption.*

Amendment 12

Proposal for a regulation Recital 22

(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.*

(22) The methods used for providing information and obtaining end-user's consent should be *clear and* user-friendly. 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 *technical* settings of a browser or other application 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, *which help them* to control the flow of information to and from the terminal equipment, *should be binding on, and enforceable against, unauthorised parties. In addition, in the light of the pace of innovation, the increasing use and range of devices that permit communications and the increase in cross-device tracking, it is necessary for this Regulation to remain technology neutral to meet its objectives.*

Amendment 13

Proposal for a regulation

Recital 23

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to ‘accept all cookies’. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option **to prevent third parties from storing information on the terminal equipment; this is often presented as ‘reject third party cookies’**. End-users should be offered a set of privacy setting options, ranging from higher (for example, ‘never accept cookies’) to lower (for example, ‘always accept cookies’) and intermediate **(for example, ‘reject third party cookies’ or ‘only accept first party cookies’)**. Such privacy settings should be presented in 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’, **which prevents end-users from providing informed and freely given consent, overloading them with requests**. Therefore providers of software enabling the retrieval and presentation of information on the internet should **inform end-users of the possibility to express their consent using appropriate technical settings. For that purpose, they should** have an obligation to configure the software so that it offers the option **for end-users to choose whether to reject or to accept trackers or cookies that are not necessary for the provision of the service requested by the end-user, after being informed of the function of the trackers or cookies, how they are used, and how the information gathered is shared**. End-users should be offered a set of privacy setting options, ranging from higher (for example, ‘never accept **trackers and** cookies’) to lower (for example, ‘always accept **trackers and** cookies’) and intermediate **options according to the types of information they are willing to share, the parties they agree to share it with, the purposes of a cookie or tracker. It should also provide them with the options to customise their settings by accepting trackers or cookies for whitelisted information society services’**. End-users should also have the possibility to opt out from cross-device tracking. **Where the end-user accepts cookies for the purpose of targeted advertising, the end-user should also be able to correct the information gathered about him or her to prevent the possible harm caused by inaccurate information**. Privacy settings should be presented in an **objective**, easily visible and intelligible manner.

Amendment 14

Proposal for a regulation Recital 23 a (new)

Text proposed by the Commission

Amendment

(23a) In order to improve trust between end-users and parties concerned with the processing of information stored in terminal equipment, and to limit the amount of tracking that negatively impacts privacy, the ability for end-users to develop their own profile, with for instance self-authored tools, should be promoted as an alternative to tracking.

Amendment 15

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

(24) For web browsers ***or other applications*** to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, 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 ***tracking cookies or other tracking mechanisms*** in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select cookies ***or trackers that process data beyond what is necessary for the service to function*** to confirm their agreement, ***after they have been provided with different options and have been*** given the necessary information to make the choice. ***Such information should include the possible impact on the customer experience or on the end-user's ability to access all the***

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.

functionalities of the website. Consent should not be valid for cross-device tracking if the end-user was not informed and is not able to opt out. 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 *tracking cookies or other tracking mechanisms* 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 *or other applications should* 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 *parties or cookies that* are always or never allowed. *Where a business model is based on targeted advertising, consent should not be considered as freely given if access to the service is made conditional on data processing. In such cases, the end-user should be provided with other fair and reasonable options that do not process his or her communications data, such as i.e. subscription, paid access, or limited access to parts of the service.*

Amendment 16

Proposal for a regulation Recital 25

Text proposed by the Commission

(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection

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 personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should ***display prominent notices located on the edge of the area of coverage informing*** end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.

with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices. ***Providers engaged in such practices should ask for the consent of the end-users concerned, after providing them with information, through a notification to their terminal equipment,*** 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. ***Where it is not possible to obtain end-user consent, such practices should be limited to what is strictly necessary for the purpose of statistical counting and should be limited***

in time and space. The data should be made anonymous or erased as soon as it is no longer needed for this purpose.

Amendment 17

Proposal for a regulation

Recital 26

Text proposed by the Commission

(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation ***should provide for*** the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, ***public security*** and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security ***and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.***

Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union

Amendment

(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation ***is without prejudice to*** the possibility for the Union or Member States under specific conditions ***set out in this regulation*** 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, 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. 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, ***following a court order and*** in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative

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).

designated pursuant to Article 3(3).

Amendment 18

Proposal for a regulation

Recital 26 a (new)

Text proposed by the Commission

Amendment

(26a) In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design. Member States should not impose any obligation on encryption providers, on providers of electronic communications services or on any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of "backdoors".

Amendment 19

Proposal for a regulation

Recital 30

Text proposed by the Commission

Amendment

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The

right to privacy and to protection of the personal data of a natural person requires that end-users that are natural persons are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.

right to privacy and to protection of the personal data of a natural person ***acting out of his/her business capacity*** requires that end-users that are natural persons are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities ***and natural persons acting in their business capacity*** requires that end-users that are legal entities ***and natural persons acting in their business capacity*** have the right to object to the data related to them being included in a directory. ***In cases where the information was not originally collected for the purposes of a publicly available directory, the first party to collect the data should be the one to request the consent of the end-user concerned. Consent should be collected by the electronic communications service provider at the moment of signing the contract for such service.***

Amendment 20

Proposal for a regulation Recital 31

Text proposed by the Commission

(31) If end-users that are natural persons give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, ***providers of publicly available directories*** should ***inform the end-users*** of the purposes of the directory and of the search functions of the directory before including them in that directory. End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the

Amendment

(31) If end-users that are natural persons give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, ***upon giving their consent the end-users*** should ***be informed*** of the purposes of the directory and of the search functions of the directory before including them in that directory. End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the

end-user's contact details can be searched should not necessarily be the same.

end-user's contact details can be searched should not necessarily be the same. ***The providers of publicly available directories should provide information about the search options, as well as if new options and functions of the directories are available in the publicly available directories.***

Amendment 21

Proposal for a regulation

Recital 37

Text proposed by the Commission

(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.***

Amendment

(37) Service providers who offer electronic communications services should ***comply with the security obligations laid down in Article 32 of Regulation (EU) 2016/679 and Article 40 of [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code]. Providers of electronic communications services should in particular ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data and that the confidentiality and integrity of the communication are guaranteed by state of the art technical measures, such as cryptographic methods, including end-to-end encryption of the electronic communications data.***

Amendment 22

Proposal for a regulation

Recital 41

Text proposed by the Commission

(41) In order to ***fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their***

Amendment

(41) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when

right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016⁸. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

⁸ ***Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016 (OJ L 123, 12.5.2016, p. 1–14).***

Amendment 23

Proposal for a regulation Article 1 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. This Regulation ensures ***the accurate and sustainable functioning of the digital single market and the*** 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.

Justification

Regulation of the Digital Single Market is needed in order to put safeguards in place.

Amendment 24

Proposal for a regulation Article 1 – paragraph 3

Text proposed by the Commission

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.

Amendment

3. The provisions of this Regulation ***does not lower the level of protection enjoyed by natural persons under the Regulation (EU) 2016/679 but*** particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.

Amendment 25

Proposal for a regulation Article 2 – paragraph 1

Text proposed by the Commission

Amendment

1. This Regulation applies to the processing of electronic communications data carried out ***in connection with the provision and the use of electronic communications*** services and to information related to the terminal equipment of end-users.

1. This Regulation applies to the processing of electronic communications data carried out ***when making available and utilizing electronic communications services, network*** services, and to information related to the terminal equipment of end-users.

Justification

There should be a distinct mentioning of "electronic communication services" and "network services", in order to ensure a level-playing field.

Amendment 26

**Proposal for a regulation
Article 3 – paragraph 2**

Text proposed by the Commission

Amendment

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 is not established in the Union it shall designate, ***and prior to the start of its activity within the Union,*** in writing a representative in the Union.

Amendment 27

**Proposal for a regulation
Article 4 – paragraph 2**

Text proposed by the Commission

Amendment

2. ***For the purposes of point (b) of paragraph 1, the definition of 'interpersonal communications service' shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.***

deleted

Amendment 28

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

Text proposed by the Commission

(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.;

Amendment

(f) ‘direct marketing communications’ means any form of advertising, whether *in* written, *audio, video, oral or any other format, sent, broadcast, served or presented* to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;

Amendment 29

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

Text proposed by the Commission

(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems;

Amendment

(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems; *this shall not include calls and text messages linked to Amber Alert;*

Justification

Amber Alert - The European Child Rescue Alert and Police Network on Missing Children, as supported by the European Parliament' Written Declaration 7/2016

Amendment 30

Proposal for a regulation
Chapter 2 – title

Text proposed by the Commission

PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT

Amendment

PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN, ***PROCESSED BY AND RELATED TO***

Amendment 31**Proposal for a regulation
Article 5 – paragraph 1***Text proposed by the Commission*

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.

Amendment

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 of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.

Amendment 32**Proposal for a regulation
Article 6***Text proposed by the Commission*

Article 6

Permitted processing of electronic communications data

1. Providers of electronic communications networks and services may process electronic communications data if:

- (a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or
- (b) it is necessary **to maintain or restore** the security of electronic communications **networks and services**, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

Amendment

Article 6

Permitted processing of electronic communications data

1. Providers of electronic communications networks and services may process electronic communications data if:

- (a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or
- (b) it is **strictly necessary for the purpose of ensuring** the security **of the net work or services or to maintain, restore or ensure the availability, security, integrity, confidentiality or authenticity** of electronic communications, or **to** detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose;

2. Providers of electronic communications services may process electronic communications metadata if:

(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) **2015/2120**²⁸ for the duration necessary for that purpose; or

(b) it is necessary for billing, **calculating** interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(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

2. Providers of electronic communications services **and network providers** may process electronic communications metadata if:

(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) **2015/2120**²⁸ for the duration necessary for that purpose, or

(a a) it is necessary in order to locate an individual following a call to emergency services, including for an Amber Alert, even if the end-user has denied or not given consent for his or her metadata to be processed, provided that the location data is strictly used for that purpose and is erased as soon as it is no longer needed for the purpose of the transmission of a communication ; or

(b) it is necessary for billing, interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing **data** that is made anonymous; **or**

(c a) the processing of the data for another specified purpose is compatible with the purpose for which the data were initially collected and is subject to specific safeguards, especially pseudonymisation, as set forth in Article 6(4) of Regulation (EU) 2016/679.

3. Providers of electronic communications services **and network providers** 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.

²⁸ 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).

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, *for the duration necessary for that purpose, provided that* the provision of that *specific* service cannot be fulfilled without the processing of such content *by the provider*;

(a a) for the sole purpose of the provision of a specific service explicitly requested by an end-user in the course of a purely personal usage or household activity, if he or she has consented to the processing of his or her electronic communications content, and that service cannot be provided without the processing of such content, where such processing produces effects solely in relation to the end-user who requested the service and does not adversely affect the fundamental rights of other users ; 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.

²⁸ 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 33

Proposal for a regulation

Article 7

Text proposed by the Commission

Article 7

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

2. Without prejudice to point (b) of Article 6(1) and points (a) **and** (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the **relevant** metadata may be kept 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

Article 7

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of Article 6(1) and points (a), **(aa)** and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or, make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

2. Without prejudice to point (b) of Article 6(1) and points (a), **(c) and (ca)** 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), **only** the metadata ***that is strictly necessary for this purpose*** 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 34

Proposal for a regulation

Article 8

Article 8

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

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

- (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
- (b) the end-user has given his or her consent; or
- (b) the end-user has given his or her consent; or
- (c) it is necessary for providing an information society service requested by the end-user; or
- (d) *if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.*

Article 8

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

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

- (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
- (b) the end-user has given his or her consent; or
- (b) the end-user has given his or her consent; or
- (c) it is necessary for providing an information society service requested by the end-user ***for the duration necessary for that provision of the service*** ; or
- (d) it is necessary ***in order to obtain information about the quality or effectiveness of an information society service that has been delivered or about terminal equipment functionality, and it has no or little impact on the privacy of the end-user concerned.***
 - (d a) it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, in particular by means of updates, or to detect technical faults or errors, for the duration necessary for that purpose, provided that:***
 - i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;***

The collection of information emitted by terminal equipment to enable it to connect to another device **and**, or to network equipment shall be prohibited, except if:

- (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or
- (b) **a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.**

The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, **have been applied.**

3. The information to be provided pursuant to point (b) of paragraph 2 may

ii) the user is informed in advance each time an update is being installed; and

iii) the user has the possibility to postpone or turn off the automatic installation of any updates.

The collection of information emitted by terminal equipment to enable it to connect to another device or to network equipment shall be prohibited, except if:

- (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or
- (b) **the end-user has given his or her consent after being informed, by way of a notification to his or her terminal equipment, of the purpose of the collection of information including the modalities of the collection, 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; or**

(b a) it is strictly necessary for the purpose of statistical counting, is limited in time and space to the extent strictly necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose in such a way that it can no longer be linked to the terminal equipment or used to single out end-users on the basis of their terminal equipment, and is only further processed for statistical purposes that generate aggregate information.

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.

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.

Amendment 35

Proposal for a regulation

Article 9

Text proposed by the Commission

Article 9

Consent

1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) **2016/679/EU** shall apply.

2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.

3. End-users who have consented to the processing of electronic

Amendment

Article 9

Consent

1. The definition of and conditions for ***informed*** consent provided for under Articles 4(11) and 7 of Regulation (EU) **2016/679** 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.

Where the user expresses consent by means of such technical settings, those settings shall be binding on, and enforceable against any other party. Where access to a service requires processing of information that is not strictly necessary for the provision of the service and an end-user has refused to give his or her consent to such processing, the end-user shall be given other fair and reasonable options to access the service.

3. End-users who have consented to the processing of electronic

communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 **and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.**

communications data as set out in point (c) of Article 6(2) and points (a), **(aa)** 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. **It shall be as easy to withdraw as to give consent.**

Amendment 36

Proposal for a regulation Article 10

Text proposed by the Commission

Article 10

Information and options for privacy settings to be provided

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

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

Amendment

Article 10

Information and options for privacy settings to be provided

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the **appropriate technical settings referred to in Article 9(2)**. **Such settings shall provide by design the** option to prevent **other** parties from **making use of the processing and storage capabilities of** the terminal equipment of an end-user or **collecting** information **from**, that equipment **that is not necessary for the provision of the specific service requested by the end-user**.

The software referred to in the first subparagraph shall offer the option to opt out from cross-device tracking.

2. The software shall inform the end-user about the privacy settings options **upon installation and after any update to the software that affects the storing of information on the terminal equipment of the end-user or the processing of information already stored on that equipment**.

Privacy settings options shall be presented in such a way as to allow the end-user to

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**.

take a fully informed decision.

Privacy settings options shall be easily accessible and modifiable during the use of the terminal equipment or software.

The European Data Protection Board shall issue guidelines on the fulfilment of the conditions of consent by appropriate technical settings by 25 November 2018.

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 November 2019**.

Amendment 37

Proposal for a regulation Article 11

Text proposed by the Commission

Article 11

Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests ***referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.***

Amendment

Article 11

Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the ***following*** general public interests:

(a) ***national security;***

(b) ***defence;***

(c) ***the prevention, investigation, detection or prosecution of serious criminal offences or the execution of***

criminal penalties, including the safeguarding against and the prevention of threats to public security.

In particular, any legislative measure restricting the scope of obligations and rights provided for in Article 5 shall contain specific provisions, where relevant, pursuant to Article 23(2) of Regulation (EU) 2016/679 and be implemented on the basis a court order.

In accordance with Article 17, no legislative measure referred to in paragraph 1 may allow for the weakening of the cryptographic methods used or the security and integrity of the terminal equipment, or the communication networks and services.

2. Providers of electronic communications services shall ***establish internal procedures for responding to*** requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. ***They shall provide the competent supervisory authority, on demand, with information about those procedures,*** the number of requests received, the legal justification invoked ***and their response.***

2. Providers of electronic communications services shall ***provide on demand, to the competent supervisory authority and to the public, information about*** requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1 ***in particular*** the number of requests received, the ***number of requests granted, and the*** legal justification invoked.

Amendment 38

Proposal for a regulation Article 13 – paragraph 1

Text proposed by the Commission

1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification ***and the denial or absence of consent of an end-user for the processing***

Amendment

1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification, on a per-line basis for organisations dealing with emergency

of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.

communications, including public safety answering points, for the purpose of responding to such communications.

Justification

Deleted and moved to Art. 6., par. 2a (new)

Amendment 39

Proposal for a regulation

Article 13 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1 a. This Regulation shall be without prejudice to the requirements for the deployment of the eCall in-vehicle system based on the 112 service (Regulation 2015/758) and shall allow eCall to handle emergency situations and carry out the tasks as effectively as possible;

Amendment 40

Proposal for a regulation

Article 14 – paragraph 1 – point a

Text proposed by the Commission

Amendment

(a) to block incoming calls from specific numbers or from anonymous sources;

(a) to block incoming calls from specific numbers or ***numbers having a specific code or prefix identifying the fact that the call is a marketing call referred to in Article 16(3)(b),*** or from anonymous sources;

Amendment 41

Proposal for a regulation

Article 15

Article 15

Publicly available directories

1. The providers of **publicly available directories** shall obtain the consent of end-users who are natural persons to **include** their personal data **in the directory** and, consequently, shall **obtain consent from these** end-users **for** inclusion of data per category of personal data, to the extent that such data are **relevant** for the purpose of **the directory as determined by the provider** of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.

2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.

3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.

4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.

Article 15

Publicly available directories

1. The providers of **electronic communication services** shall obtain the consent of end-users who are natural persons to **share** their personal data **with the providers of publicly available directories** and, consequently, shall **provide** end-users **with information about** inclusion of data per category of personal data, to the extent that such data are **necessary** for the purpose of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.

2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.

3. The **providers of electronic communication services or** providers of publicly available directories shall provide end-users that are legal persons **or natural persons acting in a business capacity** 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 **or natural persons acting in a business capacity** 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 **and in an easily accessible manner by the provider of electronic communication services or directly from the provider of publicly available directory.**

4 a. Where the personal data of end-

users who are natural persons have been included in a publicly available directory before this Regulation enters into force, and where acquiring consent would lay an unreasonable burden on the directory or originating service provider, the personal data of such end-users may remain included in a publicly available directory, including versions with search functions, unless the end-users have expressed their manifest objection against their data being included in the directory or against available search functions related to their data.

Amendment 42

Proposal for a regulation Article 16

Text proposed by the Commission

Article 16

Unsolicited communications

1. Natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons *that* have given their consent.

2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own *similar* products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.

3. Without prejudice to paragraphs 1

Amendment

Article 16

Unsolicited communications

1. Natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons *and* have given their consent.

2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own 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 *customer shall be informed of 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.

3. Without prejudice to paragraphs 1

and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:

(a) present the identity of a line on which they can be contacted; or

(b) present a specific code/or prefix identifying the fact that the call is a marketing call.

4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.

5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected.

6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, *in an easy manner*, to receiving further marketing communications.

and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:

(a) present the identity of a line on which they can be contacted; or

(b) present a specific code/or prefix identifying the fact that the call is a marketing call.

4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications. ***Member States shall provide that users can object to receiving the unsolicited communications via a national Do Not Call Register, thereby also ensuring that the user is only required to opt out once.***

5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected.

6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent ***or to object free of charge, as provided for in Article 12(5) of Regulation (EU) No 2016/679***, to receiving further marketing communications. ***Any use of masked sender identities, false contact information or false return addresses or numbers for direct marketing purposes***

7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.

Amendment 43

Proposal for a regulation Article 17

Text proposed by the Commission

Article 17

Information about detected security risks

In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.

shall be prohibited.

7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.

Amendment

Article 17

Security obligations

Providers of electronic communication services shall comply with the security obligations as set out in Regulation (EU) 2016/679 and [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code]. Providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data and that the confidentiality and integrity of the communication are guaranteed by state of the art technical measures, including cryptographic methods such as end-to-end encryption.

In order to provide information to end-users about security standards, self-certification or labelling schemes specifying the security and quality characteristics of software and terminal equipment shall be promoted.

Amendment 44

Proposal for a regulation Article 19 – paragraph 1 – point b a (new)

Text proposed by the Commission

Amendment

(ba) draw up guidelines for supervisory authorities concerning the application of Article 9(1) and the particularities of expression of consent by legal entities;

Amendment 45

Proposal for a regulation

Article 21 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. An end-user or a group of end-users shall have the right to mandate a non-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of protection of their personal data and the protection of privacy to lodge the complaint on his or her behalf, to exercise the rights referred to in paragraphs 1 and 2 of this Article on his or her behalf, and to exercise the right to receive compensation referred to in Article 22 on his or her behalf where provided for by Member State law.

Amendment 46

Proposal for a regulation

Article 21 – paragraph 2 b (new)

Text proposed by the Commission

Amendment

2b. A body, organisation or association independently of the end-user's mandate, shall have the right to lodge, in the Member State where it is registered, a complaint with the supervisory authority which is competent pursuant to paragraph 1 of this Article and to exercise the rights referred to in paragraph 2 of this Article if it considers

that the rights of the end-user under this Regulation have been infringed.

Amendment 47

**Proposal for a regulation
Chapter VI – title**

Text proposed by the Commission

Amendment

**DELEGATED ACTS AND
IMPLEMENTING ACTS**

IMPLEMENTING ACTS

Amendment 48

**Proposal for a regulation
Article 25**

Text proposed by the Commission

Amendment

Article 25

deleted

Exercise of the delegation

- 1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.***
- 2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation].***
- 3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.***
- 4. Before adopting a delegated act, the Commission shall consult experts***

designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Amendment 49

Proposal for a regulation Article 27

Text proposed by the Commission

Article 27

Repeal

1. Directive 2002/58/EC is repealed with effect from 25 *May* 2018.
2. References to the repealed Directive shall be construed as references to this Regulation.

Amendment

Article 27

Repeal

1. Directive 2002/58/EC is repealed with effect from 25 *November* 2018.
2. References to the repealed Directive shall be construed as references to this Regulation.

Amendment 50

Proposal for a regulation Article 28

Text proposed by the Commission

Article 28

Monitoring and evaluation clause

By 1 **January** 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.

No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.

Amendment 51

Proposal for a regulation

Article 29

Text proposed by the Commission

Article 29

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from 25 **May** 2018.

Amendment

Article 28

Monitoring and evaluation clause

By 1 **June** 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.

No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.

Amendment

Article 29

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from 25 **November** 2018.

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	ITRE 16.2.2017
Rapporteur Date appointed	Kaja Kallas 16.3.2017
Discussed in committee	21.6.2017
Date adopted	2.10.2017
Result of final vote	+: 50 –: 5 0: 7
Members present for the final vote	Nikolay Barekov, Nicolas Bay, Bendt Bendtsen, Xabier Benito Ziluaga, José Blanco López, David Borrelli, Jonathan Bullock, Cristian-Silviu Buşoi, Edward Czesak, Jakop Dalunde, Pilar del Castillo Vera, Fredrick Federley, Adam Gierek, Theresa Griffin, Rebecca Harms, Hans-Olaf Henkel, Kaja Kallas, Barbara Kappel, Krišjānis Kariņš, Seán Kelly, Jaromír Kohlíček, Peter Kouroumbashev, Zdzisław Krasnodębski, Miapetra Kumpula-Natri, Christelle Lechevalier, Janusz Lewandowski, Paloma López Bermejo, Edouard Martin, Angelika Mlinar, Csaba Molnár, Nadine Morano, Dan Nica, Aldo Patriciello, Miroslav Poche, Michel Reimon, Massimiliano Salini, Algirdas Saudargas, Sven Schulze, Neoklis Sylikiotis, Dario Tamburrano, Patrizia Toia, Evžen Tošenovský, Claude Turmes, Vladimir Urutchev, Kathleen Van Brempt, Henna Virkkunen, Martina Werner, Lieve Wierinck, Anna Záborská, Carlos Zorrinho
Substitutes present for the final vote	Pilar Ayuso, Pervenche Berès, Michał Boni, Rosa D'Amato, Jens Geier, Françoise Grossetête, Werner Langen, Olle Ludvigsson, Răzvan Popa, Dennis Radtke, Dominique Riquet
Substitutes under Rule 200(2) present for the final vote	Claudia Schmidt

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

50	+
ALDE	Fredrick Federley, Kaja Kallas, Angelika Mlinar, Dominique Riquet, Lieve Wierinck
ECR	Nikolay Barekov, Edward Czesak, Hans-Olaf Henkel, Zdzisław Krasnodębski, Evžen Tošenovský
ENF	Nicolas Bay, Barbara Kappel, Christelle Lechevalier
PPE	Pilar Ayuso, Bendt Bendtsen, Michał Boni, Cristian-Silviu Bușoi, Françoise Grossetête, Krišjānis Kariņš, Seán Kelly, Werner Langen, Janusz Lewandowski, Nadine Morano, Aldo Patriciello, Dennis Radtke, Massimiliano Salini, Algirdas Saudargas, Claudia Schmidt, Sven Schulze, Vladimir Urutchev, Henna Virkkunen, Anna Záborská, Pilar del Castillo Vera
S&D	Pervenche Berès, José Blanco López, Jens Geier, Adam Gierek, Theresa Griffin, Peter Kouroumbashev, Miapetra Kumpula-Natri, Olle Ludvigsson, Edouard Martin, Csaba Molnár, Dan Nica, Miroslav Poche, Răzvan Popa, Patrizia Toia, Kathleen Van Brempt, Martina Werner, Carlos Zorrinho

5	-
EFDD	Jonathan Bullock
GUE	Xabier Benito Ziluaga, Jaromír Kohlíček, Paloma López Bermejo, Neoklis Sylikiotis

7	0
EFDD	David Borrelli, Rosa D'Amato, Dario Tamburrano
Verts/ALE	Jakop Dalunde, Rebecca Harms, Michel Reimon, Claude Turmes

Key to symbols:

+ : in favour

- : against

0 : abstention

6.10.2017

OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

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: Eva Maydell

SHORT JUSTIFICATION

The protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector is one of the main pillars of the Digital Single Market (DSM) Strategy, and so is to guarantee the free movement of electronic communications data, equipment and services in the Union in order to provide a level playing field for all market players.

The current Commission's proposal aims to achieve these goals, by reviewing the e-Privacy Directive. Ahead of the coming into effect of the General Data Protection Regulation 2016/679 (GDPR) it is important to ensure consistency between the different legal instruments addressing personal data in the digital environment, with the objective to increase trust in and the security of digital services in the DSM.

Your rapporteur welcomes the proposal as an important part of the DSM Strategy, but believes that in order to achieve its main objectives different changes are needed.

First of all your rapporteur believes that the proposal should only clarify the provisions of GDPR and fill the regulatory gaps where they exist, but should not go beyond the requirements of the GDPR creating additional barriers and burdens.

The proposal should therefore facilitate and help commercial and social activities online, the legislative framework in this field should allow and provide a proper business environment for the creation of new products and services thus increasing the competition and giving the access to more choice and services for consumers.

Overregulation and complex procedures that impede the evolution of the DSM and the satisfaction of end-users' demands, would be highly counterproductive and burdensome for European consumers and businesses. Therefore, consumer-friendly digital environment

should be at the core of this proposal in order to provide for informed choice of privacy settings.

To achieve this goal several amendments of the rapporteur are addressing, inter alia, the broad reference to machine-to-machine communications and the unclear extent of the exemption of corporate networks. In addition, the rapporteur believes that amendments are necessary to provide for more flexibility for the permitted processing of information based on consent.

In Article 3, on the territorial scope and representative, an amendment is introduced to avoid duplication of regulation. The GDPR imposes a requirement on providers of electronic communications services not established within the Union to designate a representative.

In Article 4, on definitions, the rapporteur believes that this regulation must be aligned with the proposed Directive on establishing the European Electronic Communications Code, in order to insure a consistent treatment of ‘ancillary services’ across the legal instruments of the DSM Strategy.

In Article 5, on the confidentiality of electronic communications data, the rapporteur believes that processing of data has been extensively covered by Article 6 in the current proposal for regulation and also in the GDPR.

In Article 6, regarding the permitted processing of electronic communications data, metadata and content, your rapporteur believes that a simplification of the text is necessary. The rapporteur considers that processing of previously collected data for compatible purposes, such as the development of services that ultimately provide added value for the end-users and their user-experience, public authorities and businesses should be allowed.

The rapporteur proposes the deletion of Article 7 because the storage and later use of communications data of natural persons are covered under the GDPR. As proposed, Article 7 would require immediate deletion of communications data after transmission with only a few limited exceptions. With the advent of digital communications using audio, text and video components, service providers often need to store message content for later use, such as allowing the user to access old communication and messages. Such practices will already be subject to the GDPR’s limitations on the storage and later use of end users’ personal data.

In Article 10, the rapporteur opposes mandatory choice making, but believes in an open scheme that allows and simplifies the end-users’ experience. Freedom of choice should always be guaranteed but it should not be made compulsory. In Article 11, on Restrictions, some amendments are tabled to clarify the responsibilities and obligations of the providers.

In Article 15, the rapporteur believes that the providers of electronic services are in best position to obtain the consent of the end-user regarding the inclusion of their data in public directories. In Article 16, the rapporteur believes that the proposed two measures serve different purpose. While it is essential to present the identity of the contact line, an obligation of a prefix may be disproportionate additional costs for the natural and legal persons, especially micro enterprises and start-ups.

Finally, in Article 17, the rapporteur believes that it is of end-users’ best interest to be made aware of possible serious risks of security breach, especially with the increase of global cyber-security threats.

AMENDMENTS

The Committee on the Internal Market and Consumer Protection 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 2

Text proposed by the Commission

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

Amendment

(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing conclusions to be drawn regarding the private lives of the persons involved in the electronic communication. ***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 2

Proposal for a regulation

Recital 6

Text proposed by the Commission

(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council⁵ remain generally sound, that Directive has not fully kept pace with the evolution of

Amendment

(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council⁵ 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.

⁵ 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 3

Proposal for a regulation

Recital 8

Text proposed by the Commission

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

technological and market reality, resulting in an *insufficient clarity and enforcement of the* 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 *users*, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.

⁵ 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

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

Amendment 4

Proposal for a regulation

Recital 11

Text proposed by the Commission

(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 Code²⁴]. 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.

²⁴ Commission proposal for a Directive of the European Parliament and of the

Amendment

(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. ***This Regulation aims at ensuring*** an effective and equal protection of end-users when using functionally equivalent services, ***so as to ensure the confidentiality of their communication, irrespective of the technological medium chosen.*** ***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 Code²⁴]. 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.

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)).

Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

Amendment 5

Proposal for a regulation

Recital 12

Text proposed by the Commission

(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. ***Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.***

Amendment

(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. ***Nevertheless, in the context of automated supply-chains and elsewhere in the manufacturing or industrial context, where communication by the machines involved is not inter-personal and does not involve natural persons, this Regulation should not apply.***

Amendment 6

Proposal for a regulation

Recital 13

Text proposed by the Commission

(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks

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.***

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. ***Therefore, this Regulation should apply to electronic communications data using electronic communications services which are targeting the general public, and public communications networks. In addition, this Regulation should also apply to closed social media profiles and groups that the user has restricted or defined as private. This Regulation should not apply to other kind of closed groups such as corporate networks, access to which is limited to members of the corporation. Such networks are offered to a defined group of end-users. However, even if undefined end-users use the network in question in the context of the activities of the defined group of end-users it should not preclude them from being considered outside the material scope of the Regulation. For example, an enterprise's collaboration platform primarily used by its employees that allows third parties to call-in or otherwise engage in the workspace should not be covered. The mere act of requiring a password should not be considered as providing access to a closed group of end-users if the access is provided to an undefined group of end-users.***

Amendment 7

Proposal for a regulation

Recital 16

Text proposed by the Commission

(16) The prohibition of storage of communications is not intended to prohibit

Amendment

(16) The prohibition of storage of communications ***during transmission*** is

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.

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. ***This Regulation also*** should not prohibit either the processing of electronic communications data to ensure the security, ***confidentiality, integrity, availability, authenticity*** and continuity of the electronic communications services ***and networks***, including checking security threats ***related to the respective service*** or the processing of metadata ***of the respective service*** to ensure the necessary quality of service requirements, such as latency, jitter etc.

Amendment 8

Proposal for a regulation

Recital 16 a (new)

Text proposed by the Commission

Amendment

(16a) Regulation (EU) 2016/679 of the European Parliament and of the Council^{1a} explicitly recognises the need to provide additional protection to children, given that they may be less aware of the risks and consequences associated with the processing of their personal data. This Regulation should also grant special attention to the protection of children's privacy. They are among the most active internet users and their exposure to profiling and behaviourally targeted advertising techniques should be prohibited.

^{1a} Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) (OJ L 119,

Amendment 9

Proposal for a regulation

Recital 17

Text proposed by the Commission

(17) The processing of electronic communications **data** can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, **based on end-users consent**. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to **obtain end-users' consent to process** electronic communications metadata, which should include data on the location of the device **generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing** electronic communications services **should not be considered as** metadata. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous

Amendment

(17) The processing of electronic communications **metadata** 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 **further** process electronic communications metadata. 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 **comply with Regulation (EU) 2016/679 when processing** electronic communications metadata, which should include data on the location of the device. **The processing of** electronic communications metadata **for purposes other than those for which the personal data were initially collected should be allowed in cases where consent was obtained for the initial collection and the further processing is compatible in accordance with Article 6(4) of Regulation (EU) 2016/679**. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of

data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. *Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.*

Amendment 10

Proposal for a regulation Recital 19

Text proposed by the Commission

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to *adequate* safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. *Given the sensitivity of the content of communications, this*

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.

Amendment

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. *For services that are provided to users engaged in purely personal,*

Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the *end-user* and received by the intended *end-user or end-users*, it may be recorded or stored by the *end-user, end-users* or by *a third* party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.

household or business activities, the consent of the end-user requesting the service should be sufficient. Where an electronic communication service that is based on new technologies is likely to result in a high risk to the rights and freedoms of natural persons after taking into account the nature, scope, context and purposes of the service the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The obligation does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing. After electronic communications content has been sent by the sender and received by the intended recipient(s), it may be recorded or stored by the sender, the recipient(s) or by another party entrusted by them to record or store such data. For communications, which do not happen in real time, such as email and messaging, the transmission is completed as soon as the communication is delivered to the trusted service provider or collected by the addressee. Any processing of such data must comply with Regulation (EU) 2016/679. **It should be possible to process electronic communications data for the purposes of providing services requested by a user for personal or work-related purposes such as search or keyword indexing functionality, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools for instance by persons with disabilities. This should be possible without the consent of all users who are part of the communication, but may take place with the consent of the user requesting the service. Such specific consent also precludes the provider from processing those data for different**

purposes.

Amendment 11

Proposal for a regulation Recital 21

Text proposed by the Commission

(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.

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, ***or processed by,*** terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy, ***for*** instance the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a service requested by the end-user. This may include the storing of ***information (such as cookies and identifiers)*** 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. ***This may also cover situations where end-users use a service across devices for the purpose of service personalisation and content recommendation.*** Cookies, ***if implemented with appropriate privacy safeguards,*** can also be a legitimate and useful tool, for example, in measuring web traffic to a website. ***Such measuring could also be carried out by another party which acts as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service. Similarly, providers of terminal equipment and the software needed to operate such equipment regularly need access to configuration and other device information and the processing and storage capabilities to maintain the equipment or its use, and correct problems related to the equipment's operation. Therefore, consent should also***

not be necessary if the information processed or stored is necessary to protect privacy, security or safety of the end-user, or to protect confidentiality, integrity, availability and authenticity of the terminal equipment. Information society providers and electronic communications service 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 user's device is unable to receive content requested by the end-user should not constitute *illegitimate* access.

Amendment 12

Proposal for a regulation Recital 22

Text proposed by the Commission

(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

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 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 *or to object* by appropriate *technical* settings. 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, *unauthorised* parties, *provided that there is no separate specific consent given by the end-user*. Web browsers are a type of software application that permits the retrieval and presentation of information on

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.*

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. *On the other hand, in light of the pace of innovation, the increasing use and range of devices that permit communications and the increase of cross-device tracking, it is necessary for this Regulation to remain technology neutral to meet its objectives.* More particularly web browsers, *applications or mobile operating systems should not abuse their position as gate-keepers and still allow for possibilities for the user to individually give consent with regard to a certain specific service or service provider. Such consent should prevail over the privacy settings chosen at an earlier date or at the point of installation of the software.*

Amendment 13

Proposal for a regulation Recital 23

Text proposed by the Commission

(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

Amendment

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to *inform the end-user about the possibility to express or withdraw his or her consent using appropriate technical settings. The end-user should be offered multiple options to choose from, including to prevent the storage of information on the terminal equipment.* End-users should be offered a set of

offered a set of privacy setting options, ranging from *higher* (for example, ‘*never accept cookies*’) to *lower* (for example, ‘*always accept cookies*’) and *intermediate* (for example, ‘*reject third party cookies*’ or ‘*only accept first party cookies*’). Such privacy settings should be presented in *a* an easily visible and intelligible manner.

privacy setting options, ranging from, for example, *rejecting cookies or trackers that are not necessary for the functionality of the website or other software to*, for example, *accepting tracking necessary for the functionality of the website or other software as well as for other purposes or, for example, accepting tracking necessary for the functionality of the website or other software and tracking for other purposes by parties that demonstrate the compliance with Article 40 and 42 of Regulation (EU) 2016/679, and the possibility to opt out from cross-device tracking. These options may also be more fine-grained and, among other aspects, reflect the possibility that another party might act as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service. In cases where a business model is based on targeted advertising, consent should not be considered as freely given if the access to the service is made conditional on data processing. The end-user should therefore be able to choose between accepting cookies or being provided fair and reasonable options to access the service, such as subscription, payment or limited access to parts of the service or other options. Where the end-user accepts cookies for purpose of targeted advertising, the end-user should also be able to correct the information gathered about him or her to prevent the possible harm caused by inaccurate information.* Such privacy settings should be presented in an easily visible and intelligible manner. *Information provided may include examples of benefits and risks associated with allowing cookies to be stored in the computer. Such obligations do not arise where the software already seeks to prevent the storage of information on the terminal equipment of an end-user or the processing of information already stored on that equipment.*

Amendment 14

Proposal for a regulation Recital 23 a (new)

Text proposed by the Commission

Amendment

(23a) Children merit specific protection with regard to their online privacy. They usually start using the internet at an early age and become very active users. Yet, they may be less aware of the risks and consequences associated to their online activities, as well as less aware of their rights. Specific safeguards are necessary in relation to the use of children's data, notably for the purposes of marketing and the creation of personality or user profiles.

Amendment 15

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

deleted

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.

Amendment 16

Proposal for a regulation

Recital 25

Text proposed by the Commission

(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

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 personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.

scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should ***ask for the end-user's consent, or where consent is not possible, such practices should be limited to what is strictly necessary for the purpose of statistical counting, be limited in time and space, or should carry out data protection impact assessment and in this case the data collected is or is rendered pseudonymous or anonymous or erased as soon as it is no longer needed for this purpose. Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, prior consultation with the supervisory authority, as prescribed in Article 36 of Regulation (EU) 2016/679, should be carried out. Providers should display or make available*** 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.

Amendment 17

Proposal for a regulation Recital 26

Text proposed by the Commission

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

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 ***is targeted at persons suspected of having committed a criminal offence and*** constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 27 of ***Regulation (EU) 2016/679. Providers of electronic communications services should not be obliged by Union or Member States competent authorities to weaken any measures that ensure the integrity and confidentiality of electronic***

authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).

communications.

Amendment 18

Proposal for a regulation Recital 26 a (new)

Text proposed by the Commission

Amendment

(26a) In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design. Member States should not impose any obligation on encryption providers, on providers of electronic communications services or on any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of "backdoors".

Amendment 19

Proposal for a regulation Recital 30

Text proposed by the Commission

Amendment

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person requires that end-users that are natural persons ***are asked for consent before their personal data are*** included in a directory. The

(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person ***acting in a professional capacity*** requires that end-users that are natural persons ***provided with transparent information about the data***

legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.

being included in the directory and the means to verify, correct, update, supplement and delete data relating to them free of charge, as well as the possibility of objecting to their data being included in public directories. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.

Amendment 20

Proposal for a regulation

Recital 31

Text proposed by the Commission

(31) If end-users that are natural persons ***give their consent to*** their data being included in such directories, they should be able to ***determine on a consent basis*** which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, providers of publicly available directories should inform the end-users of the purposes of the directory and of the search functions of the directory ***before including them in that directory. End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the end-user's contact details can be searched should not necessarily be the same.***

Amendment

(31) If end-users that are natural persons ***do not object to*** their data being included in such directories, they should be able to ***make an objection on*** which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, providers of publicly available directories ***or the providers of electronic communications services*** should inform the end-users of the purposes of the directory and of the search functions of the directory.

Amendment 21

Proposal for a regulation

Recital 33

(33) Safeguards should be provided to protect end-users against unsolicited communications for direct marketing purposes, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, emails, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent level of protection for all citizens throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of *similar* products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.

(33) Safeguards should be provided to protect end-users against unsolicited communications, *including* 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 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.

Amendment 22

Proposal for a regulation Recital 37

(37) Service providers who offer electronic communications services should **inform end- users** of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679.

(37) Service providers who offer electronic communications services should **process electronic communications data in such a way as to prevent unauthorised processing, including access, disclosure or alteration. They should ensure that such unauthorised access, disclosure or alteration is possible of being ascertained, and also ensure that electronic communications data are protected by using state of the art software and encryption technologies. Service providers should also inform end-users** of measures they can take to protect **their anonymity and** 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.

Amendment 23

Proposal for a regulation Recital 39

(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the

(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the

powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.

powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. ***Supervisory authorities should cooperate with the relevant authorities in other enforcement areas as appropriate.***

Amendment 24

Proposal for a regulation Recital 40

Text proposed by the Commission

(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.

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. ***Double penalties resulting from the infringement of both this Regulation and Regulation (EU)***

2016/679 for the same act or omission should be avoided.

Amendment 25

Proposal for a regulation Recital 41

Text proposed by the Commission

(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016²⁵. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

Amendment

(41) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

²⁵ ***Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016 (OJ L 123, 12.5.2016, p. 1–14).***

Amendment 26

Proposal for a regulation

Recital 43

Text proposed by the Commission

(43) Directive 2002/58/EC should be repealed.

Amendment

(43) Directive 2002/58/EC **and Commission Regulation (EU) 611/2013^{1a}** should be repealed.

^{1a} ***Commission Regulation (EU) 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (OJ L 173, 26.6.2013, p. 2).***

Justification

The Commission Regulation (EU) 611/2013 setting out specific rules on data breach notifications should be repealed as its legal basis, Directive 2002/58/EC, will be repealed, and the GDPR will apply for breach notifications.

Amendment 27

Proposal for a regulation

Article 1 – paragraph 2

Text proposed by the Commission

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.***

Amendment

2. This Regulation ensures, ***in accordance with Regulation (EU) 2016/679***, free movement of electronic communications data and electronic communications services within the Union.

Amendment 28

**Proposal for a regulation
Article 1 – paragraph 3**

Text proposed by the Commission

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.

Amendment

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. ***Regulation (EU) 2016/679 applies to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Regulation, including the obligations on the controller and the rights of individuals.***

Amendment 29

**Proposal for a regulation
Article 2 – paragraph 1**

Text proposed by the Commission

1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services ***and to information related to the terminal***

Amendment

1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services.

equipment of end-users.

Amendment 30

Proposal for a regulation Article 3 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. Where the provider of an electronic communications service is not established in the Union ***the party identified pursuant to Article 27 of Regulation (EU) 2016/679 shall act as its*** representative in the Union.

Amendment 31

Proposal for a regulation Article 3 – paragraph 3

Text proposed by the Commission

3. ***The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.***

Amendment

deleted

Amendment 32

Proposal for a regulation Article 5 – paragraph 1

Text proposed by the Commission

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.

Amendment

Electronic communications data shall be confidential. Any interference with electronic communications data ***during transmission***, such as by listening, tapping, storing, or other kinds of interception, ***or*** surveillance of electronic communications data, by persons other than the ***sender or intended recipients***, shall be prohibited, except when permitted by this Regulation.

Amendment 33

Proposal for a regulation

Article 6 – title

Text proposed by the Commission

Permitted processing of electronic communications data

Amendment

Lawful processing of electronic communications data

Amendment 34

Proposal for a regulation

Article 6 – paragraph 1

Text proposed by the Commission

1. Providers of electronic communications networks and services may process electronic communications data if:

(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or

(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

Amendment

1. Providers of ***public*** electronic communications networks and ***publicly available electronic communications*** services may process electronic communications data if:

(a) it is ***technically*** necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or

(b) it is ***technically*** necessary to maintain or restore the ***availability, integrity, security and confidentiality of the respective*** electronic communications networks and services, or ***to*** detect technical faults and/or errors in the transmission of electronic communications, ***or to stop fraudulent use of the service*** for the duration necessary for that purpose.

Amendment 35

Proposal for a regulation

Article 6 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. Electronic communications data that is generated in the context of an electronic communications service

designed particularly for children or directly targeted at children shall not be used for profiling or behaviourally targeted advertising purposes.

Amendment 36

Proposal for a regulation Article 6 – paragraph 2

Text proposed by the Commission

2. Providers of electronic communications services may process electronic communications metadata if:
- (a) it is necessary *to meet mandatory* quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120²⁸ for the duration necessary for that purpose; or
- (b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or
- (c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

Amendment

2. Providers of electronic communications *networks and* services may process electronic communications metadata if:
- (a) it is necessary *for quality of service purposes, including network management and* quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120²⁸ for the duration necessary for that purpose; or
- (b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or
- (ba) the further processing of the metadata for another specified purpose is compatible with the purpose for which the data were initially collected and is subject to specific safeguards, especially pseudonymisation, as set forth in Article 6(4) of Regulation (EU) 2016/679;*
- (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.

²⁸ 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).

²⁸ 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 37

Proposal for a regulation Article 6 – paragraph 3

Text proposed by the Commission

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.***

Amendment

3. Providers of the electronic communications services may process electronic communications content:
- (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 ***service providers' end-users have consented*** to the processing of their electronic communications content ***pursuant to Regulation (EU) 2016/679; or***
- (ba) for the sole purpose of the provision of a specific service explicitly requested by an end-user in the course of a purely personal, household or business***

activity, if the end-user concerned has consented to the processing of his or her electronic communications content and that service cannot be provided without the processing of such content.

Amendment 38

Proposal for a regulation Article 7 – paragraph 1

Text proposed by the Commission

1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a *third* party entrusted by *them* to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

Amendment

1. Without prejudice to point (b) of Article 6(1) and points (a), *(aa)* 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 party, *which could be the provider of the electronic communication service, specifically* entrusted by *the end-user* to record, store or otherwise process such data. *The end-user may further process the content* in accordance with Regulation (EU) 2016/679, *if applicable*.

Amendment 39

Proposal for a regulation Article 7 – paragraph 2

Text proposed by the Commission

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.

Amendment

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 *or pseudonymous* when it is no longer needed for the purpose of the transmission of a communication.

Amendment 40

Proposal for a regulation Article 8 – paragraph 1

Text proposed by the Commission

1. The use of processing and storage capabilities of terminal equipment and the collection of **information** from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

- (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
- (b) the end-user has given his or her consent; or
- (c) it is necessary for providing **an information society** service requested by the end-user; or
- (d) if it is necessary for **web** audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.

Amendment

1. The use of processing and storage capabilities of terminal equipment and the collection of **personal data** from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

- (a) it is **technically** necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
- (b) the end-user has given his or her consent; or
- (c) it is necessary for providing **a service** requested by the end-user ***especially in order to secure the integrity, security and access of the information society service or for measures to protect against unauthorised use or access to the information society services in agreement with the terms of use for making available the service to the end-user;*** or
- (d) if it is necessary for audience measuring, provided that such measurement is carried out by, ***or on behalf of*** the provider of the information society service requested by the end-user, ***including measurement of indicators for the use of information society services in order to calculate a payment due, and provided that such audience measurement does not adversely affect the fundamental rights of the end-user or it is necessary in order to obtain information about the technical quality or effectiveness of an information society service that has been delivered and has no or little impact on***

the privacy of the end-user concerned. Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers; or

(da) it is necessary to protect privacy, security or safety of the end-user, or to protect confidentiality, integrity, availability, authenticity of the terminal equipment.

Amendment 41

Proposal for a regulation Article 8 – paragraph 2

Text proposed by the Commission

2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or

(b) a clear and prominent notice *is displayed informing of*, at least, the modalities of the 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

Amendment

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 *sole* purpose of establishing a connection *requested by the user*; or

(ab) the data are anonymised and the risks are adequately mitigated; or

(ac) it is necessary for the purpose of statistical counting, which is limited in time and space to the extent strictly necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose.

(b) *the end-user has given his or her consent after being informed by* a clear and prominent notice *for*, 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

take to stop or minimise the collection.

The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

the end-user of the terminal equipment can take to stop or minimise the collection.

The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

Amendment 42

Proposal for a regulation Article 8 – paragraph 3

Text proposed by the Commission

Amendment

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.*

deleted

Amendment 43

Proposal for a regulation Article 8 – paragraph 4

Text proposed by the Commission

Amendment

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.*

deleted

Amendment 44

Proposal for a regulation Article 8 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4 a. *Terminal equipment that is intended particularly for children's use shall implement specific measures to prevent access to the equipment's storage and processing capabilities for the purpose of profiling of its users or tracking their behaviour with commercial intent.*

Amendment 45

Proposal for a regulation

Article 9 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. *Where access to a service requires processing of information that is not strictly necessary for the provision of the service and an end-user has refused to give his or her consent to such processing, the end-user shall be given other fair and reasonable options to access the service.*

Amendment 46

Proposal for a regulation

Article 9 – paragraph 3

Text proposed by the Commission

Amendment

3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 **and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.**

3. End-users who have consented to the processing of electronic communications data as set out in point (c) of 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. **It shall be as easy to withdraw as to give consent.**

Amendment 47

Proposal for a regulation

Article 10 – paragraph 1

Text proposed by the Commission

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.

Amendment

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 ***the storage of*** information on the terminal equipment of an end-user or ***the processing of*** information already stored on that equipment.

Amendment 48

Proposal for a regulation

Article 10 – paragraph 2

Text proposed by the Commission

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.***

Amendment

2. Upon installation, the software shall inform the end-user about the privacy settings options. ***The technical settings shall consist of multiple options for the end-user to choose from, including an option to prevent the storage of information on the terminal equipment of an end-user and the processing of information already stored on, or processed by, that equipment. These settings shall be easily accessible during the use of the software.***

Amendment 49

Proposal for a regulation

Article 10 – paragraph 3

Text proposed by the Commission

3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2

Amendment

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**.

shall be complied with at the time of the first update of the software, but no later than ***one year after entry into force of this Regulation***.

Amendment 50

Proposal for a regulation Article 11 – paragraph 1

Text proposed by the Commission

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard ***one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.***

Amendment

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 ***national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences.***

Amendment 51

Proposal for a regulation Article 11 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. Member States law may not require the removal or the corruption of technical protection measures, such as end-to-end encryption; nor should it otherwise determine the nature of such measures, where these are applied directly by the provider of the electronic communications network, service or terminal equipment, or by the end-user.

Amendment 52

Proposal for a regulation

Article 12 – paragraph 1 – introductory part

Text proposed by the Commission

1. Where presentation of the calling and connected line identification is offered in accordance with Article [107] of the [Directive establishing the European Electronic Communication Code], the providers of publicly available number-based interpersonal communications services shall provide the following:

Amendment

1. Where presentation of the calling and connected line identification is offered in accordance with Article [107] of the [Directive establishing the European Electronic Communication Code], the providers of publicly available number-based interpersonal communications services shall provide the following, ***subject to technical feasibility and economic viability:***

Amendment 53

Proposal for a regulation

Article 15 – paragraph 1

Text proposed by the Commission

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.***

Amendment

1. ***Without prejudice to Member States national law the providers of electronic information, communication and telecommunication services shall give end-users who are natural persons the right to object to data related to them being included in directories and shall provide a transparent information about the data being included in the directory and the means to verify, correct, update and delete such data.***

Amendment 54

Proposal for a regulation

Article 15 – paragraph 2

Text proposed by the Commission

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.

Amendment

2. The providers of a publicly available directory shall **provide accessible and intelligible information to** end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and **provide** end-users' **the option to disable** such search functions related to their own data.

Amendment 55

Proposal for a regulation
Article 15 – paragraph 3

Text proposed by the Commission

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.

Amendment

3. The providers of **electronic information, communications and telecommunications services** 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, **update, supplement** and delete such data. **Natural persons acting in a professional capacity, such as independent professionals, operators of small businesses or freelancers, shall be equated with legal persons.**

Amendment 56

Proposal for a regulation
Article 15 – paragraph 4

Text proposed by the Commission

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

Amendment

4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct, **update, supplement** and delete any data related to them shall be provided free of charge **and**

free of charge.

in an easily accessible manner.

Amendment 57

Proposal for a regulation

Article 15 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. *The provisions of paragraphs 1 to 4 shall not apply to data and information published in other publicly accessible sources and data provided by end-users themselves, nor shall it apply to data published in publicly available directories before this Regulation enters into force unless the end-users have expressed their objection against their data being included in the directory or against available search functions related to their data pursuant to Article 17 of Regulation (EU) 2016/679.*

Amendment 58

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 **electronic mail** from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own **similar** products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.

2. Where a natural or legal person obtains electronic contact details for **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 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 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 59

Proposal for a regulation Article 16 – paragraph 3

Text proposed by the Commission

3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:

(a) *present the identity of a line on which they can be contacted; or*

(b) *present a specific code/or prefix identifying the fact that the call is a marketing call.*

Amendment 60

Proposal for a regulation Article 16 – paragraph 4

Text proposed by the Commission

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.

Amendment 61

Proposal for a regulation Article 17

PE606.011v02-00

184/245

RR\1137482EN.docx

Amendment

3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall *present the identity of a line on which they can be contacted and may present a specific code/or prefix identifying the fact that the call is a marketing call.*

Amendment

4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users shall only be allowed in respect of end-users who have not expressed their objection to receiving those communications. *Member States may provide that users can object to receiving the unsolicited communications via a national Do Not Call Register, thereby also ensuring that the end-user is only required to opt out once.*

Article 17

deleted

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.

Amendment 62

Proposal for a regulation

Article 18 – paragraph 1

Text proposed by the Commission

Amendment

1. ***The independent supervisory authority or*** authorities responsible for monitoring the application of ***Regulation (EU) 2016/679 shall also be responsible for monitoring the application of*** this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.

1. ***Each Member State shall provide that one or more independent public*** authorities ***are*** responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.

Amendment 63

Proposal for a regulation

Article 18 – paragraph 2

Text proposed by the Commission

Amendment

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

2. ***Each supervisory authority shall contribute to the consistent implementation of this Regulation throughout the Union.*** The supervisory authority or authorities referred to in

European Electronic Communications Code].

paragraph 1 shall cooperate whenever appropriate with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code] **and the national authorities responsible for monitoring the implementation of consumer protection legislation (Regulation (EU) .../... of the European Parliament and of the Council^{1a})**.

^{1a} **Regulation (EU) .../... of the European Parliament and of the Council of ... on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) 2006/2004 (OJ ...)**.

Amendment 64

Proposal for a regulation Article 21 – paragraph 2

Text proposed by the Commission

Amendment

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.

deleted

Amendment 65

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

deleted

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.

Amendment 66

Proposal for a regulation Chapter 6 – title

Text proposed by the Commission

Amendment

**DELEGATED ACTS AND
IMPLEMENTING ACTS**

IMPLEMENTING ACTS

Amendment 67

Proposal for a regulation Article 25

Text proposed by the Commission

Amendment

Article 25

deleted

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation].

3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the

European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Amendment 68

Proposal for a regulation Article 27 – paragraph 1

Text proposed by the Commission

1. Directive 2002/58/EC is repealed with effect from **25 May 2018**.

Amendment

1. Directive 2002/58/EC **and Regulation 611/2013 are** repealed with effect from **[XXX]**.

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	IMCO 16.2.2017
Rapporteur Date appointed	Eva Maydell 9.2.2017
Discussed in committee	4.9.2017 25.9.2017
Date adopted	28.9.2017
Result of final vote	+: 19 -: 13 0: 5
Members present for the final vote	John Stuart Agnew, Pascal Arimont, Dita Charanzová, Carlos Coelho, Sergio Gaetano Cofferati, Anna Maria Corazza Bildt, Daniel Dalton, Nicola Danti, Pascal Durand, Evelyne Gebhardt, Maria Grapini, Robert Jarosław Iwaszkiewicz, Liisa Jaakonsaari, Philippe Juvin, Antonio López-Istúriz White, Jiří Maštálka, Eva Maydell, Marlene Mizzi, Nosheena Mobarik, Jiří Pospíšil, Marcus Pretzell, Virginie Rozière, Christel Schaldemose, Olga Sehnalová, Igor Šoltes, Ivan Štefanec, Catherine Stihler, Mihai Țurcanu, Anneleen Van Bossuyt, Marco Zullo
Substitutes present for the final vote	Lucy Anderson, Edward Czesak, Kaja Kallas, Adam Szejnfeld, Matthijs van Miltenburg, Lambert van Nistelrooij
Substitutes under Rule 200(2) present for the final vote	Vladimir Urutchev

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

19	+
ALDE	Dita Charanzová, Kaja Kallas, Matthijs van Miltenburg
ECR	Edward Czesak, Daniel Dalton, Nosheena Mobarik, Anneleen Van Bossuyt
PPE	Pascal Arimont, Carlos Coelho, Anna Maria Corazza Bildt, Philippe Juvin, Antonio López-Istúriz White, Eva Maydell, Jiří Pospíšil, Adam Szejnfeld, Vladimir Urutchev, Lambert van Nistelrooij, Ivan Štefanec, Mihai Țurcanu

13	-
EFDD	John Stuart Agnew
GUE/NGL	Jiří Maštálka
S&D	Lucy Anderson, Sergio Gaetano Cofferati, Nicola Danti, Evelyne Gebhardt, Maria Grapini, Liisa Jaakonsaari, Marlene Mizzi, Virginie Rozière, Christel Schaldemose, Olga Sehnalová, Catherine Stihler

5	0
EFDD	Robert Jarosław Iwaszkiewicz, Marco Zullo
ENF	Marcus Pretzell
Verts/ALE	Pascal Durand, Igor Šoltes

Key to symbols:

+ : in favour

- : against

0 : abstention

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

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

Commission proposal

(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

Amended text

(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***

and personal messaging provided through social media.

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

Commission proposal

(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.

Amended text

(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. ***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

Commission proposal

(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.

Amended text

(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

Commission proposal

(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council²² 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.

Amended text

(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council²² 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

Commission proposal

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

Amended text

deleted

Amendment 6

Proposal for a regulation

Recital 9

Commission proposal

(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.

Amended text

(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.

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

Commission proposal

(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 Code²⁴]. 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,

Amended text

(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 Code²⁴]. 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***

such type of services also having a communication functionality should be covered by this Regulation.

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

Commission proposal

(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

Amended text

(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

Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.

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

Commission proposal

(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.

Amended text

(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. ***It should also include location data, such as for example the actual or inferred location of the terminal equipment, the location of the terminal equipment from or to which a phone call or an internet connection has been made, or the Wi-Fi hotspot that a device is connected to, as well as data necessary to identify 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)

Commission proposal

Amended text

(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

Commission proposal

Amended text

(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

(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

communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.

electronic communications, 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

Commission proposal

(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

Amended text

(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***

etc.

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

Commission proposal

(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

Amended text

(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 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.

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.

Amendment 14

Proposal for a regulation Recital 20

Commission proposal

(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

Amended text

(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of

Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes.

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 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

Commission proposal

(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.***

Amended text

(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website ***by the person or legal person in charge of the website ("first party analytics")***.

Amendment 16

Proposal for a regulation

Recital 21 a (new)

Commission proposal

Amended text

(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

Commission proposal

(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

Amended text

(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should *prevent the use of so-called "cookie walls" and "cookie banners" that 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

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.

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

Commission proposal

(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

Amended text

(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*

easily visible and intelligible manner.

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

Commission proposal

(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

Amended text

deleted

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.

Amendment 20

Proposal for a regulation

Recital 25

Commission proposal

(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

Amended text

(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.

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. ***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

Commission proposal

(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

Amended text

(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,

prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).

detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. ***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)

(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

Commission proposal

(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

Amended text

(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.

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

Commission proposal

(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.

Amended text

(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 **and** present a specific code identifying the fact that the call is a marketing call.

Amendment 25

Proposal for a regulation Recital 37

Commission proposal

(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

Amended text

(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**

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.

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

Commission proposal

(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

Amended text

(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.

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

Commission proposal

Article 1

Subject matter

1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.

2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, which shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data.

3. The provisions of this Regulation ***particularise and*** complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.

Amended text

Article 1

Subject matter

1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.

2. This Regulation ensures, ***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 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***

Amendment 28

Proposal for a regulation
Article 2

Commission proposal

Article 2

Material Scope

1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.

2. This Regulation does not apply to:

- (a) activities which fall outside the scope of Union law;
- (b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;
- (c) electronic communications services which are not publicly available;
- (d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of

Amended text

Article 2

Material Scope

1. This Regulation applies to :

(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 ***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/EC¹, 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).

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/EC¹, 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).

Amendment 29

Proposal for a regulation Article 3

Commission proposal

Article 3

Territorial scope and representative

1. This Regulation applies to:

(a) ***the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;***

Amended text

Article 3

Territorial scope and representative

1. This Regulation applies to ***the activities referred to in Article 2 where the end user is in the Union:***

- (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.

3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.

4. The representative shall *have the power* to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to *processing electronic communications data* for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against a natural or legal person who *processes electronic communications data in connection with the provision of electronic communications services* from outside the Union to end-users in the Union.

2. Where the provider of an electronic communications service, *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.

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 *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

Commission proposal

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;

Amended text

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

Commission proposal

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.;

Amended text

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

Commission proposal

PROTECTION OF ELECTRONIC

Amended text

PROTECTION OF ELECTRONIC

Amendment 33

Proposal for a regulation
Article 5

Commission proposal

Article 5

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.

Amended text

Article 5

Confidentiality of electronic
communications data

Confidentiality of electronic
communications data

I. 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 of 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.***

Ib. 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

Commission proposal

Article 6

Permitted processing of electronic communications data

Permitted processing of electronic communications data

1. Providers of electronic communications networks and services may process electronic communications data if:

(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or

(b) it is necessary to maintain or restore ***the*** security of electronic communications networks ***and*** services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

Amended text

Article 6

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 ***only***:

(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) 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

2. Providers of electronic communications services may process electronic communications metadata if:

(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120¹ for the duration necessary for that purpose; or

(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled **by processing information that is made anonymous**.

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

processing of such metadata.

2. Providers of electronic communications services may process electronic communications metadata **only**:

(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) 2015/2120¹ for the duration **technically** necessary for that purpose; or

(b) if it is **strictly** necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive **unlawful** use of, or subscription to, electronic communications services; or

(c) ***after receiving all relevant information about the intended processing in 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.

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

Commission proposal

Article 7

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of Article 6(1) **and** points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept 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

Amended text

Article 7

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of Article 6(1), points (a) **and (c) of Article 6(2) and points (a)** and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications 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 process such data in accordance with Regulation (EU) 2016/679.

2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), **the 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.

Article 8

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

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(b) the end-user *has* given *his or her* consent; *or*

(c) it is necessary for providing an information society service requested by the end-user; or

(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society *service requested by* the end-user.

Article 8

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, ***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 ***strictly*** necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network ***whereby the data shall be stored in a binary format***; 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 ***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 ***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 exist.

(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:

(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or

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 *sole* purpose of establishing a connection

(b) a clear and ***prominent notice is displayed informing of***, at least, ***the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.***

The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

3. The information to be provided

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) ***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.

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.

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.

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.

Amendment 37

Proposal for a regulation

Article 9

Commission proposal

Article 9

Consent

1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.

2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using *the appropriate technical settings of a software application enabling access to the internet*.

3. End-users who have *consented* to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 *and* be reminded of this possibility at periodic intervals of 6 months, as long as the processing

Amended text

Article 9

Consent

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, *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 *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,*

continues.

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

Commission proposal

Article 10

Information and options for privacy settings to be provided

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.

Amended text

Article 10

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:

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.*

3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.

2. *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 than 25 August 2018.

Amendment 39

Proposal for a regulation Article 10 a (new)

Commission proposal

Amended text

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

Commission proposal

Article 11

Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.

2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. **They** shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

Amended text

Article 11

Restrictions

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 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. ***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

Commission proposal

Article 15

Publicly available directories

1. The providers of publicly available directories shall obtain ***the*** consent of end-users who are natural persons to include their personal data in the directory ***and, consequently, shall obtain consent from these end-users for inclusion of*** data per ***category of personal data***, to the extent that such data are relevant for the purpose of the directory ***as determined by the provider of the directory***. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.
2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data.
3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such

Amended text

Article 15

Publicly available directories

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.
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.

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.

Amendment 42

Proposal for a regulation Article 16– paragraph 1

Commission proposal

(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.

Amended text

(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

Commission proposal

(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,

Amended text

(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

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.

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

Commission proposal

a) present the identity of a line on which they can be contacted; ***or***

Amended text

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)

Commission proposal

Amended text

(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

Commission proposal

(4) Notwithstanding paragraph 1, Member States may provide by law that

Amended text

deleted

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.

Amendment 47

Proposal for a regulation Article 16 – paragraph 6

Commission proposal

(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.

Amended text

(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

Commission proposal

Article 17

Information about detected security risks
In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall *inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an*

Amended text

Article 17

Information about detected security risks
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*

indication of the likely costs involved.

European Electronic Communications Code.

Amendment 49

Proposal for a regulation

Article 21

Commission proposal

Article 21

Remedies

1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679.
2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation and having a legitimate interest in the cessation or prohibition of alleged infringements, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.

Amended text

Article 21

Remedies

1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 **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.

Amendment 50

Proposal for a regulation

Article 22 – paragraph 1

Commission proposal

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

Amended text

Article 82 of Regulation (EU) No 2016/679 **shall apply.**

for the event giving rise to the damage in accordance with Article 82 of Regulation (EU) 2016/679.

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**

Commission proposal

Amended text

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)**

Commission proposal

Amended text

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**

Commission proposal

Amended text

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)

Commission proposal

Amended text

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

Commission proposal

(2) The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for ***an indeterminate period of time*** from [the data of entering into force of this Regulation].

Amended text

(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].

Amendment 56

Proposal for a regulation Article 28 – paragraph 1

Commission proposal

By 1 January 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.

Amended text

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

PROCEDURE – COMMITTEE RESPONSIBLE

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)			
Date submitted to Parliament	12.1.2017			
Committee responsible Date announced in plenary	LIBE 16.2.2017			
Committees asked for opinions Date announced in plenary	ENVI 16.2.2017	ITRE 16.2.2017	IMCO 16.2.2017	JURI 16.2.2017
Not delivering opinions Date of decision	ENVI 31.1.2017			
Rapporteurs Date appointed	Marju Lauristin 9.3.2017			
Discussed in committee	8.6.2017	21.6.2017	28.9.2017	19.10.2017
Date adopted	19.10.2017			
Result of final vote	+ : 31 - : 24 0 : 1			
Members present for the final vote	Asim Ahmedov Ademov, Jan Philipp Albrecht, Gerard Batten, Heinz K. Becker, Michał Boni, Caterina Chinnici, Daniel Dalton, Rachida Dati, Cornelia Ernst, Laura Ferrara, Raymond Finch, Ana Gomes, Nathalie Griesbeck, Sylvie Guillaume, Jussi Halla-aho, Monika Hohlmeier, Sophia in 't Veld, Eva Joly, Dietmar Köster, Barbara Kudrycka, Cécile Kashetu Kyenge, Marju Lauristin, Juan Fernando López Aguilar, Monica Macovei, Roberta Metsola, Claude Moraes, Alessandra Mussolini, József Nagy, Péter Niedermüller, Soraya Post, Judith Sargentini, Birgit Sippel, Csaba Sógor, Helga Stevens, Traian Ungureanu, Bodil Valero, Harald Vilimsky, Kristina Winberg, Tomáš Zdechovský, Auke Zijlstra			
Substitutes present for the final vote	Anna Maria Corazza Bildt, Ignazio Corrao, Dennis de Jong, Gérard Deprez, Lívia Járóka, Sylvia-Yvonne Kaufmann, Andrejs Mamikins, Angelika Mlinar, Kati Piri, Jaromír Štětina, Axel Voss			
Substitutes under Rule 200(2) present for the final vote	Xabier Benito Ziluaga, Josu Juaristi Abaunz, Kaja Kallas, Martin Sonneborn, Janusz Zemke			
Date tabled	23.10.2017			

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

31	+
ALDE	Gérard Deprez, Nathalie Griesbeck, Sophia in 't Veld, Kaja Kallas, Angelika Mlinar
EFDD	Ignazio Corrao, Laura Ferrara
GUE/NGL	Xabier Benito Ziluaga, Cornelia Ernst, Josu Juaristi Abaunz, Dennis de Jong
NI	Martin Sonneborn
S&D	Caterina Chinnici, Ana Gomes, Sylvie Guillaume, Sylvia-Yvonne Kaufmann, Cécile Kashetu Kyenge, Dietmar Köster, Marju Lauristin, Juan Fernando López Aguilar, Andrejs Mamikins, Claude Moraes, Péter Niedermüller, Kati Piri, Soraya Post, Birgit Sippel, Janusz Zemke
Verts/ALE	Jan Philipp Albrecht, Eva Joly, Judith Sargentini, Bodil Valero

24	-
ECR	Daniel Dalton, Jussi Halla-aho, Monica Macovei, Helga Stevens
EFDD	Gerard Batten, Raymond Finch
ENF	Harald Vilimsky, Auke Zijlstra
PPE	Asim Ahmedov Ademov, Heinz K. Becker, Michał Boni, Anna Maria Corazza Bildt, Rachida Dati, Monika Hohlmeier, Lívia Járóka, Barbara Kudrycka, Roberta Metsola, Alessandra Mussolini, József Nagy, Csaba Sógor, Jaromír Štětina, Traian Ungureanu, Axel Voss, Tomáš Zdechovský

1	0
EFDD	Kristina Winberg

Key to symbols:

+ : in favour

- : against

0 : abstention