European Parliament
2014-2019

Committee on Legal Affairs

2017/0003(COD)

10.7.2017

AMENDMENTS
43 - 193

Draft opinion
Axel Voss
(PE605.986v01-00)

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)

Proposal for a regulation
(COM(2017)0010 – C8-0009/2017 – 2017/0003(COD))

AM_Com_LegOpinion

Amendment 43
Gilles Lebreton, Marie-Christine Boutonnet

Proposal for a regulation
Title 1

Text proposed by the Commission	*Amendment*
Proposal for a	Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	***DIRECTIVE*** 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)***	concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

Or. fr

Amendment 44
Daniel Buda

Proposal for a regulation
Recital 1

Text proposed by the Commission	*Amendment*
(1) Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the parties involved in a communication. The principle of confidentiality should apply to current and future means of communication, including	(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 ***confidential*** communications. Respect for the privacy ***and confidentiality*** 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.	calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media. ***Effective protection of the confidentiality of communications is essential for exercising the freedom of expression and information and other rights enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms.***

Or. ro

Amendment 45
Max Andersson

Proposal for a regulation
Recital 1

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

Or. en

Amendment 46
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 1

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

Or. en

Amendment 47
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication,	(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.

from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc. ***The protection of confidentiality of communications is an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, freedom of assembly, freedom of expression and information.***

Or. en

Amendment 48
Jean-Marie Cavada

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very	(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 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 one of the essential conditions for respect for fundamental rights and freedoms, along with the freedoms of conscience, religion and expression.***

Or. fr

Amendment 49
Mady Delvaux

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) ***The content of*** electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. ***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	(2) 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,

activities of everyday life, their interests, tastes etc.

tastes etc. ***The protection of confidentiality of communications is also an essential condition for the respect of other related fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, and freedom of expression and information.***

Or. en

Amendment 50
Daniel Buda

Proposal for a regulation
Recital 3

Text proposed by the Commission	*Amendment*
(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation ***should*** apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council[21], also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.	(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. ***The case-law of the Court of Justice of the European Union ('CJEU')[20a] and the European Court of Human Rights[20b]confirms that the professional activities of legal persons may not be excluded from the protection afforded by Article 7 of the Charter and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.*** Therefore, the provisions of this Regulation apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council[21], also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this

Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.

_____

[20a] See Case C-450/06, Varec SA, ECLI: EU:C:2008:91, paragraph 48.

[20b] See, for example, ECHR judgment Niemietz v. Germany of 16 December 1992, series A, No 251-B, paragraph 29; Société Colas Est and others v France, No 37971/97, paragraph 41; ECHR 2002-III; Peck v. United Kingdom, No 44647/98, paragraph 57, ECHR 2003-I; and Vinci Construction and GTM Génie Civil et Services v. France, Nos 63629/10 and 60567/10, paragraph 63, 2 April 2015.

[21] 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. 1–88).

[21] 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. 1–88).

Or. ro

Amendment 51
Jiří Maštálka, Kateřina Konečná

Proposal for a regulation
Recital 3

Text proposed by the Commission	*Amendment*
(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council[21],	(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that ***certain*** provisions of the Regulation (EU) 2016/679 of the European Parliament and

also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.	of the Council[21], also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.
[21] 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. 1–88).	[21] 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. 1–88).

Or. en

Amendment 52
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 5

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

permitted in accordance with this Regulation.	permitted in accordance with ***and on a legal ground specifically provided under*** this Regulation.

Or. en

Amendment 53
Max Andersson

Proposal for a regulation
Recital 5

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

Or. en

Amendment 54
Daniel Buda

Proposal for a regulation
Recital 6

Text proposed by the Commission	*Amendment*
(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[22] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting	(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting

in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of online behaviour of end-users, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.	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).

Or. ro

Amendment 55
Jens Rohde

Proposal for a regulation
Recital 6

Text proposed by the Commission	*Amendment*
(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[22] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient ***effective***	(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[22] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient protection

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).

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).

Or. en

Amendment 56
Mady Delvaux

Proposal for a regulation
Recital 7

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

communications data.

Or. en

Amendment 57
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 7

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

Or. en

Amendment 58
Daniel Buda

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(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,	(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. ***Moreover, Member States should remain free to keep or create national***

should maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.

data retention frameworks that provide, inter alia, for targeted retention measures, far as such frameworks comply with Union law, taking into account the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights[1a]. 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.

_____

[1a] See joint cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others, ECLI:EU:C:2014/238; joint cases C-203/15 and C-698/15 Tele2 Sverige AB and Secretary of State for the Home Department, ECLI:EU:C:2016:970.

Or. ro

Amendment 59
Jiří Maštálka, Kostas Chrysogonos, Kateřina Konečná

Proposal for a regulation
Recital 7

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

Or. en

Amendment 60
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 8

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

Or. en

Amendment 61
Axel Voss

Proposal for a regulation
Recital 8 a (new)

Text proposed by the Commission	*Amendment*
	(8a) This Regulation permits the processing of electronic communications data and of information conveyed to, stored in, retrieved from or otherwise processed in relation to terminal equipment to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of networks or information systems to resist, at a given level of confidence, accidental events or unlawful or malicious actions that

	compromise the availability, authenticity, integrity and confidentiality of stored or transmitted electronic communications data, and the security of the related services offered by, or accessible via, those networks and systems. Such processing is permitted for providers of electronic communications networks and services, for users, as well as for relevant third parties such as public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs) and providers of security technologies and services.

Or. en

Amendment 62
Mady Delvaux

Proposal for a regulation
Recital 9

Text proposed by the Commission	*Amendment*
(9) This Regulation should apply to electronic communications data processed in connection with the provision and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union.	(9) This Regulation should apply to electronic communications data processed in connection with the provision and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union. ***This should be the case irrespective of whether the electronic communications are connected to a payment or not.***

Or. en

Amendment 63
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 11

Text proposed by the Commission	*Amendment*
(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. In order to ensure an effective and equal protection of end-users when using functionally equivalent services, this Regulation uses the definition of electronic communications services set forth in the [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code***[24]***]. That definition encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.	(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***, full*** and equal protection of end-users when using functionally equivalent services, this Regulation uses the definition of electronic communications services set forth in the [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code***[24]***]. That definition encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service***, such as internal messaging, newsfeeds, timelines and similar functions in online services where messages are exchanged with other users within or outside that service (i.e. public and privately available newsfeeds and timelines)***; therefore, such type of services also having a communication functionality should be covered by this Regulation.
_____	_____

[24] Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

[24] Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

Or. en

Amendment 64
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 11 a (new)

Text proposed by the Commission	*Amendment*
	(11a) The definition of "end-user" should for instance include employees, tenants, hotel guests, family members, visitors, and any other individuals who are as a matter of fact using the services, for private or business purposes, without necessarily having subscribed to it.

Or. en

Amendment 65
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls ***and hospitals***. To the extent that those communications networks are provided to an undefined	(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, hospitals and other similar Internet access points***. To the extent that those

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.

communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be ***adequately*** protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.

Or. en

Amendment 66
Jiří Maštálka, Kateřina Konečná

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls ***and*** hospitals. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of	(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 protected. The fact that wireless electronic communications services may be ancillary to other services

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.

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.

Or. en

Amendment 67
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 14

Text proposed by the Commission	*Amendment*
(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services 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	(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

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.

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.

Or. en

Amendment 68
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 14

Text proposed by the Commission	*Amendment*
(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services 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)	(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***

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.

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.

Or. en

Amendment 69
Mady Delvaux

Proposal for a regulation
Recital 14

Text proposed by the Commission	*Amendment*
(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services 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	(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 specific location 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.	***such as for example the location of the terminal equipment from or to which a phone call or an internet connection has been made or the Wi-Fi access points that a device is connected to, as well as data necessary to identify the terminal equipment of 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.

Or. en

Amendment 70
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 14 a (new)

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

Or. en

Amendment 71
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.	(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. ***When the processing is allowed under any exception to the prohibitions under the this Regulation, any other processing of the electronic communications data on the basis of Article 6 of Regulation (EU) 2016/679 should be considered as prohibited, including processing for another purpose on the basis of Article 6(4) of that Regulation. This would not prevent controllers from asking for additional consent for new processing operations.*** The prohibition of interception of communications data should apply ***also*** during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee ***and any temporary files in the network after receipt***. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from

terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers***, and analysis of end users' electronic communications metadata***, including browsing habits without the end-users' consent.

Or. en

Amendment 72
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(15) ***Electronic communications data should be treated as confidential. This means that*** any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, ***without the consent of all the communicating parties should be*** prohibited. The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor	(15) ***Any processing of electronic communications data or*** any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, ***by persons other than the end-users, should be prohibited. When the processing is allowed under any exception to the prohibitions under this Regulation, any other processing of the electronic communications data on the basis of Article 6 of the Regulation (EU) 2016/679 should be considered as*** prohibited***, including processing for another purpose on the basis of Article 6(4) of that Regulation. This would not prevent controllers from asking for additional consent for new processing operations***. The prohibition of interception of communications data should apply ***also*** during their conveyance, i.e. until receipt of the content of the electronic

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.

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

Or. en

Amendment 73
Max Andersson

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human	(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human

intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.	intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of communications data should ***also*** apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee***, and when stored***. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers***, injecting ads or other content and analysis of customers´ traffic data***, including browsing habits without the end-users' consent.

Or. en

Amendment 74
Angel Dzhambazki

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., ***without the consent of the end-user concerned***. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that***, for example, surreptitiously*** monitor browsing habits ***for the purpose of creating end-user profiles***. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers***, including browsing habits without the end-users' consent***.	(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited ***except for permissible uses as set forth in this Regulation***. 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 ***or their electronic communications service providers***, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata ***during transmission*** 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., ***by accessing electronic communications data during their transmission on public communications networks***. 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 monitor browsing habits. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers.

Or. en

Amendment 75
Angel Dzhambazki

Proposal for a regulation
Recital 15 a (new)

Text proposed by the Commission	*Amendment*
	(15a) The prohibition of interception is not intended to prohibit access to electronic communications data by an electronic communications service provider or electronic communications network operator for purposes of conveying communications or for legitimate and justifiable purposes related to the operation and protection of such services and networks consistent with obligations under Regulation (EU) 2016/679, Directive (EU) 2016/1148 and Regulation (EU) 2015/2120.

Or. en

Amendment 76
Angel Dzhambazki

Proposal for a regulation
Recital 15 b (new)

Text proposed by the Commission	*Amendment*
	(15b) Providers of electronic communications networks and services now provide their end-users with enhanced features by using communications data before the provider transmits the data through a public network or after the provider has received the data from such a network. These enhanced features include speech-to-text conversion for users with disabilities, digital personal assistants using voice commands, automatic language translation, and message prioritisation and sorting. For the purposes of these service providers, electronic

communications are not in transmission once the service provider of the intended recipient has received the communications for delivery to the recipient's terminal equipment or until the service provider of the sender has sent the communication to another service provider for eventual delivery to the intended recipient.

Or. en

Amendment 77
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 16

Text proposed by the Commission	*Amendment*
(16) The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications network. It should not prohibit either the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including checking security threats such as the presence of malware or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc.	(16) The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications network. It should not prohibit either the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including checking security threats such as the presence of malware or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc. ***Where a type of processing of electronic communications data for these purposes is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.***

Or. en

Amendment 78
Angel Dzhambazki

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 ***during transmission*** 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 ***by*** the electronic communications network ***or service. This Regulation also does*** 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. Filtering of unlawful content, including child and juvenile pornography, is permissible***.

Or. en

Amendment 79
Isabella Adinolfi, Marco Zullo

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	(16) The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and ***strictly*** transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the

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.

electronic communications network. ***Therefore, by way of exception,*** 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.

Or. en

Amendment 80
Daniel Buda

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 ***during conveyance*** 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.

Or. ro

Amendment 81
Mady Delvaux

Proposal for a regulation
Recital 16 a (new)

Text proposed by the Commission	*Amendment*
	(16a) It should be possible to oblige providers of electronic communications services to ensure a certain quality of service by, for example, ensuring that the service does not suffer degradation or that the traffic is not unduly slowed down. In this regard, it may be necessary, in some limited circumstances, to analyse metadata in real time and respond to fluctuations in traffic. Certain electronic communications metadata are necessary to enable providers to correctly bill end-users for the services used and to allow end-users to verify that the cost incurred corresponds to their actual usage. The processing and storage of such data for these purposes should therefore be permitted without requiring consent by the end-user concerned. This processing includes possible processing for customer service purposes. Metadata may also be processed to detect fraudulent use, or abusive use pursuant to Directive (EU) 2013/0309. 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. Moreover, the parties involved in the processing of location data and other metadata should make public their methods of anonymisation and further aggregation, without prejudice to secrecy obligations safeguarded by law. The anonymisation method should, once the defined purposes of the processing have been fulfilled, technically prevent all

parties from singling out a user within a set of data or from linking new data collected from the users' device to the existing set of data.

Or. en

Amendment 82
Mady Delvaux

Proposal for a regulation
Recital 17

Text proposed by the Commission	*Amendment*
(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. ***Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities 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	(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. Examples of ***such*** 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***, provided that the data are immediately anonymised or anonymisation techniques are used where the user is mixed with others***. 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.

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.***

Or. en

Amendment 83
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 17

Text proposed by the Commission	*Amendment*
(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, ***based on*** end-users consent. ***However***, end-users attach	(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, ***only where there is an informed and expressed*** end-

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)

users consent. ***Indeed***, 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' ***informed and expressed*** consent to process electronic communications metadata, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata***, but rather genuine equipment location data. In any case, location data of the terminal device of a natural person is personal data and thus the processing of those data is subject to the obligations from the Regulation (EU) 2016/679. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colours to indicate the presence of individuals***. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, ***providers must comply with the obligations from Article 25 of Regulation (EU) 2016/679 in case of further processing of location data or other metadata, conduct*** a data protection impact assessment and, as the

2016/679.

case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679. ***Moreover, the parties involved in the processing of location data and other metadata should make public their methods of anonymisation and further aggregation, without prejudice to secrecy safeguarded by law. The anonymisation method must, once the defined purposes of processing have been fulfilled, technically prevent all parties from singling out an end-user within a set of data or from linking new data collected from the end-user's device to the existing set of data.***

Or. en

Amendment 84
Max Andersson

Proposal for a regulation
Recital 17

Text proposed by the Commission	*Amendment*
(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities 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	(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, based on end-users consent. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to obtain end-users' consent to process electronic communications

metadata, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using *colors* to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier ***is*** necessary to link the positions of individuals at certain time intervals. ***This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. Where a type of*** processing ***of*** electronic communications metadata***, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be***, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.	metadata, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using *colours* to indicate the presence of individuals. ***This should be done in accordance with Article 25 of Regulation (EU) 2016/679.*** To display the traffic movements in certain directions during a certain period of time, an identifier ***may be*** necessary to link the positions of individuals at certain time intervals. ***When*** processing electronic communications metadata, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.

Or. en

Amendment 85
Jens Rohde

Proposal for a regulation
Recital 17

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

to develop new infrastructure, based on the usage of and pressure on the existing structure.

Or. en

Amendment 86
Angel Dzhambazki

Proposal for a regulation
Recital 17

Text proposed by the Commission	*Amendment*
(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities 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	(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, ***pursuant to Regulation (EU) 2016/679***. 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 ***meet the requirements of Regulation (EU) 2016/79*** to process electronic communications metadata, which should include data on the location

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

Or. en

Amendment 87
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 18

Text proposed by the Commission	*Amendment*
(18) End-users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied ***against counter-performance other than money, for instance by end-users being exposed to advertisements***. For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. Basic broadband internet access and voice communications services ***are*** to be ***considered as*** essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment.	(18) End-users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied ***with remuneration paid by a third party rather than by the recipient of the service***. For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. ***Individuals depend on and financially contribute, through taxes, to public services, services that are financed directly, indirectly, totally or partially by public funds such as medical services that are essential to fully participate in a democratic society. These services ensure and strengthen the enjoyment of human rights. Without access to these services individuals cannot fully participate in their societies. Therefore, preventing access to such services unless consent is provided to processing activities that are not strictly required for the performance of these services, should be prohibited. In addition to this,*** basic broadband internet access and voice communications services***, and other electronic communications service that have or have the potential*** to be ***used widely, are in today´s societies*** 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. ***Also, the growing use and dependence of so-called 'smart' services, such as smart cars, smart***

phones and smart TVs, are increasingly essential devices for individuals to participate in our 'connected' society. Individuals often have no genuine and free choice when accessing those essential services or using those smart devices because they are unable to refuse or withdraw consent without detriment to themselves. Situations where the individual is confronted with "take it or leave it" options, for example when they face "tracking walls", leave them without a real choice. Access to these essential services or the functionality of terminal equipment should not depend on the requirement of consent to the processing of data that is not strictly necessary for the services or for the functionality requested. Intrusive processing activities, such as analysing electronic communications content, electronic communications metadata, or tracking user activity over time or across several information society services or terminal equipment, for purposes such as providing targeted advertisements cannot be considered as strictly necessary for the service or functionality requested.

Or. en

Amendment 88
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 19

Text proposed by the Commission	*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	(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.

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. ***In exceptional circumstances, communications service providers should be able to provide the means for additional processing of electronic communications data with the consent of one of the parties to a communication, on condition that this processing is for the provision of services requested by that party and that this is strictly necessary for delivering a specific functionality, in particular such services such as voice-to-text or other automatic content processing used as accessibility tools needed by persons with disabilities. Third parties providing the means for recording, storing or otherwise processing such data used by end-users in the course of a purely individual household or individual activity, as long as this activity is part of the strictly functional aspect of hardware and software which the end-user can reasonably expect (such as voice-to- text technology, or spell checkers), should process such data in accordance with Regulation (EU) 2016/679.*** Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a

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

Or. en

Amendment 89
Daniel Buda

Proposal for a regulation
Recital 19

Text proposed by the Commission	*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	(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and ***the confidentiality of*** 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

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.

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.

Or. ro

Amendment 90
Mady Delvaux

Proposal for a regulation
Recital 19 a (new)

Text proposed by the Commission	*Amendment*
	(19a) 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 only 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.

Or. en

Amendment 91
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's	(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities ***or to instigate certain technical operations or***

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.

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.

Or. en

Amendment 92
Mady Delvaux

Proposal for a regulation
Recital 20

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

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 their device***, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. 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. ***Furthermore, so-called spyware, web bugs, hidden identifiers and unwanted tracking tools can enter end-users' terminal equipment without their knowledge in order to gain access to information or to store hidden information.*** 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. ***End-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.***

Or. en

Amendment 93
Max Andersson

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the 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	(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.	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. ***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.***
	Or. en

Amendment 94
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device,	(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**.**	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. 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

Or. en

Amendment 95
Angel Dzhambazki

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another	(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.

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 ***robust*** 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 ***or on some other legitimate basis in Union or Member State law*** and for specific and transparent purposes.

Or. en

Amendment 96
Stefano Maullu

Proposal for a regulation
Recital 21

Text proposed by the Commission	*Amendment*
(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content ***requested by the end-user*** should not constitute access to such a device or use of the device processing capabilities.	(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. ***This may also cover situations where end-users use a service across devices for the purpose of service personalization and content recommendation.*** 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 ***including advertisements,*** should not constitute access to such a device or use of the device processing capabilities. ***Information society service providers should remain free to take appropriate measures in line with their respective business models, including restricting access to content when an end user uses an adblocker.***

Or. en

Amendment 97
Angel Dzhambazki

Proposal for a regulation
Recital 21

Text proposed by the Commission	*Amendment*
(21) Exceptions to the obligation to obtain consent to ***make use of the processing and storage capabilities of*** terminal equipment or to access information stored in terminal equipment should be limited to situations that ***involve no, or only very limited, intrusion of privacy***. For instance, ***consent should not be requested for authorizing*** the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a ***specific*** service ***explicitly requested by*** the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.	(21) Exceptions to the obligation to obtain consent to ***store information in*** terminal equipment or to access information stored in terminal equipment should be limited to situations that ***comply with all obligations pursuant to Regulation (EU) 2016/679***. This concerns, for instance, the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a service ***that is beneficial to*** 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. ***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, prevent security vulnerabilities and correct problems related to the equipment's operation.*** 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 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.

Or. en

Amendment 98
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 21

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

Or. en

Amendment 99
Jean-Marie Cavada

Proposal for a regulation
Recital 21

Text proposed by the Commission	*Amendment*
(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.	(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website ***or any other digital medium***. 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.

Or. fr

Amendment 100
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 21 a (new)

Text proposed by the Commission	*Amendment*
	(21a) Equipment location data can give

a very detailed and intrusive insight into an individual´s personal life or an organisation´s business and activities. Processing of location data from any source, whether electronic communications metadata or equipment location data should be conducted on the basis of clear rules.

Or. en

Amendment 101
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 21 a (new)

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

Or. en

Amendment 102
Mady Delvaux

Proposal for a regulation
Recital 22

Text proposed by the Commission	*Amendment*
(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly	(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.

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 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 103
Jiří Maštálka, Kateřina Konečná

Proposal for a regulation
Recital 22

Text proposed by the Commission	*Amendment*
(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide 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***	(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. ***Communications software*** should ***be set by default to the most privacy-friendly option***. The choices made by ***all*** end-users when establishing ***their*** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are ***one way of accessing and sending*** information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have ***similar*** capabilities.

from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

Or. en

Amendment 104
Angel Dzhambazki

Proposal for a regulation
Recital 22

Text proposed by the Commission	*Amendment*
(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide 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	(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***, absent any separate, specific consent obtained from the end-user***. 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 provide route guidance, ***may*** have also the same capabilities. ***Terminal equipment operating systems and standalone communications software do not provide these capabilities. While website providers***

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.

are ultimately responsible for honouring the technical means of consent provided through a browser's general privacy settings, web browsers mediate much of what occurs between the end-user and the website. From this perspective, they 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. ***Examples of appropriate browser settings include settings that allow users to block all cookies or only third-party cookies, and those that allow users to send a "Do Not Track" request with their browsing traffic.***

Or. en

Amendment 105
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 22

Text proposed by the Commission	*Amendment*
(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide 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	(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.***	appropriate settings of a browser or other application. ***Communications software should be set by default to the most privacy friendly option.*** 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 ***one way of accessing and sending*** information on the internet. 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.

Or. en

Amendment 106
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 23

Text proposed by the Commission	*Amendment*
(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to ‘accept all cookies’. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this	(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.

is often presented as ‘reject third party ***trackers***’. End-users should be offered a set of privacy setting options, ranging from higher (for example, ‘never accept ***trackers'***’) to lower (for example, ‘always accept ***trackers"***) and intermediate (for example, ‘reject third party ***trackers***’ or ‘only accept first party ***trackers***’). Such privacy settings should be presented in an easily visible and intelligible manner. ***For web browsers and any other software enabling access to the internet or internet-based services to be able to obtain the consent of end-users as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking, they should, among others, require a clear affirmative action from the end-user of terminal equipment to express his or her freely given, specific, informed and explicit agreement to the storage and access of 'cookies' or any other trackers in and from the terminal equipment. To this end, it is necessary to require providers of software enabling access to the internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. That information provided to the users shall not be written in a way that seeks to dissuade end-users from selecting the most privacy-friendly settings and should include relevant information about the risks associated to allowing third party trackers to be stored on the device, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising or sharing that information with third parties. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to white-list certain websites or to specify for which websites (third) party trackers are always or never allowed. In case of no***

active choice, or action from the user, web browsers and any other software enabling access to internet-based services should be set by default to ensure the highest degree of protection for the individual, including the rejection and blocking the storage of third party 'cookies' or other type of trackers.

Or. en

Amendment 107
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 23

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

should, among others, require a clear affirmative action from the end-user of terminal equipment to express his or her freely given, specific, informed and explicit agreement to the storage and access of 'cookies' or any other trackers in and from the terminal equipment. To this end, it is necessary to require providers of software enabling access to the internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. That information provided to the users shall not be written in a way that seeks to dissuade end-users from selecting the most privacy-friendly settings and should include relevant information about the risks associated to allowing third party trackers to be stored on the device, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising or sharing that information with third parties. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to white-list certain websites or to specify for which websites (third) party trackers are always or never allowed. In case of no active choice, or action from the user, web browsers and any other software enabling access to internet-based services should be set by default to ensure the highest degree of protection for the individual, including the rejection and blocking the storage of third party 'cookies' or other type of trackers.

Or. en

Amendment 108
Mady Delvaux

Proposal for a regulation
Recital 23

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

Or. en

Amendment 109
Jean-Marie Cavada

Proposal for a regulation
Recital 23

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

Or. fr

Amendment 110
Stefano Maullu

Proposal for a regulation
Recital 23

Text proposed by the Commission	*Amendment*
(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies	(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.	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 ***setting options should differentiate between cookies from third parties that have a contractual relationship with website providers and other third party cookies. Such privacy*** settings should be presented in an easily visible and intelligible manner.

Or. en

Amendment 111
Mady Delvaux

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	***deleted***

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.

Or. en

Amendment 112
Jean-Marie Cavada

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	(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.	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***, upon a specific request,*** or to specify for which websites (third) party cookies are always or never allowed.

Or. fr

Amendment 113
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 25

Text proposed by the Commission	*Amendment*
(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a	(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.

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. ***Such practices should be prevented to ensure compliance with the principle of purpose limitation as defined under Regulation (EU) 2016/679.*** While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations***. Therefore, only in a limited number of circumstances and only if the used data would be anonymised or deleted after the defined purposes of processing have been fulfilled, might data controllers be allowed to process the information emitted by the terminal equipment for the purposes of tracking the physical movements of end-users with his or her consent. The anonymisation method should technically prevent all parties from singling out an end-user within a set of data or from linking new data collected from the end-user's terminal equipment to the existing set of data***. 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.

Or. en

Amendment 114
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 25

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

to send commercial messages to end-users, for example when they enter stores, with personalized offers. 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 personalized offers. ***Such practices should be prevented to ensure compliance with the principle of purpose limitation as defined under Regulation (EU) 2016/679.***While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. ***Therefore, only in a limited number of circumstances and only if the used data would be anonymised or deleted after the defined purposes of processing have been fulfilled, might data controllers be allowed to process the information emitted by the terminal equipment for the purposes of tracing the physical movements of end-users with his or her consent. The anonymistaion method should technically prevent all parties from singling out an end-user within a set of data or from linking new data collected from the end-user´s*** terminal equipment ***to the existing set of data***. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.

Or. en

Amendment 115
Mady Delvaux

Proposal for a regulation
Recital 25

Text proposed by the Commission	*Amendment*
(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be	(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.

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. ***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.***

Or. en

Amendment 116
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 26

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

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).

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 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).

Or. en

Amendment 117
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 26

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

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

Amendment 118
Angel Dzhambazki

Proposal for a regulation
Recital 26

Text proposed by the Commission	*Amendment*
(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article ***3(3)***.	(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article ***27 of Regulation (EU) 2016/679***.

Or. en

Amendment 119
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the end-users of electronic communications services. The availability of electronic communications service options with alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example unregistered SIM cards and facilitates for payment by credit card, can mitigate these risks. When the end-user is a natural person who is different from the subscriber receiving the itemised bill, for example in an employment context, the operator of number-based interpersonal communication services should offer their subscribers a different type of itemised bill in which a certain number of digits of the called number will not be shown.

Or. en

Amendment 120
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 31

Text proposed by the Commission	*Amendment*
(31) If end-users that are natural persons	(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.

give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, providers of publicly available directories should inform the end-users of the purposes of the directory and of the search functions of the directory before including them in that directory. End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the end-user's contact details can be searched should not necessarily be the same. ***Since reverse searches of natural persons based on phone numbers or service identifiers such as email addresses or user names may be regarded as more intrusive than other searches, a separate consent should always be required before enabling such searches of the end-user.***

Or. en

Amendment 121
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 32

Text proposed by the Commission	*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***. 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	(32) In this Regulation, direct marketing refers to any form of advertising ***or similar promotion*** by which a natural or legal person sends direct ***or presents direct*** marketing communications directly to one or more identified or identifiable end-users ***over an*** electronic communications ***network***. In addition to the offering of products and services for commercial purposes, this should also include

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.	messages sent by political parties ***or members of political parties*** that contact natural persons via electronic communications services in order to promote their parties***, candidacy in elections or other political campaigns***. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.

Or. en

Amendment 122
Axel Voss

Proposal for a regulation
Recital 32

Text proposed by the Commission	*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. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.	(32) In this Regulation, direct marketing refers to any form of advertising 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. ***It should not apply to the communication for scientific research purposes like market and opinion research.***

Or. en

Amendment 123
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 32 a (new)

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

Or. en

Amendment 124
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 33

Text proposed by the Commission	*Amendment*
(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	(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***, directed or presented*** to end-users***, who are natural persons, including natural persons working for legal persons,*** in order to effectively protect individuals against the intrusion into their private life***. Member States should also ensure that*** the legitimate interest of legal persons ***with regard to***

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.

unsolicited communications are protected. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent level of protection for all ***individuals*** throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679 ***and only for a limited time period***.

Or. en

Amendment 125
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Recital 33

Text proposed by the Commission	*Amendment*
(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	(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.	purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent level of protection for all citizens throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679 ***and only for a limited time period***.

Or. en

Amendment 126
Jiří Maštálka, Kateřina Konečná

Proposal for a regulation
Recital 35

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

code identifying the fact that the call is a marketing call.	specific code identifying the fact that the call is a marketing call.

Or. en

Amendment 127
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Recital 36

Text proposed by the Commission	*Amendment*
(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish and or maintain national systems only allowing such calls to end-users who have not objected.	(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish and or maintain national systems only allowing such calls to end-users who have not objected. ***End-users should be able to object to future calls from a specific company or organization. Member States should also ensure that the end-users can object to all future voice-to-voice direct marketing calls by registering their objection in the national "Do Not Call" register. A user-friendly option to object to all future calls should be provided free of charge.***

Or. en

Amendment 128
Mady Delvaux

Proposal for a regulation
Recital 37

Text proposed by the Commission	*Amendment*
(37) Service providers who offer electronic communications services should ***inform end- users of measures they can***	(37) Service providers who offer electronic communications services should ***process electronic communications data***

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.

in such a way as to prevent unauthorised access, disclosure or alteration, ensure that such unauthorised access, disclosure or alteration is capable of being ascertained, and also ensure that such electronic communications ***data are protected*** by using specific types of software ***and*** encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679. ***The obligations of Article 40 of the [European Electronic Communications Code] should apply to all services within the scope of this Regulation as regards the security of networks and services and related security obligations thereto.***

Or. en

Amendment 129
Angel Dzhambazki

Proposal for a regulation
Recital 37

Text proposed by the Commission	*Amendment*
(37) Service providers who offer electronic communications services should inform end- users of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security ***risks*** does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to	(37) Service providers who offer ***publicly available*** electronic communications services should inform end- users of measures they can take to protect the security of their communications ***from particular and significant security threats,*** for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security ***threats*** does not discharge a service

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.

provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any security risks and restore the normal security level of the service. The provision of information about security ***threats*** to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679.

Or. en

Amendment 130
Jean-Marie Cavada

Proposal for a regulation
Recital 40

Text proposed by the Commission	*Amendment*
(40) In order to strengthen the enforcement of the rules of this Regulation, each supervisory authority should have the power to impose penalties including administrative fines for any infringement of this Regulation, in addition to, or instead of any other appropriate measures pursuant to this Regulation. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. For the purpose of setting a fine under this Regulation, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 of the Treaty.	(40) In order to strengthen the enforcement of the rules of this Regulation, each supervisory authority should have the power to impose penalties including administrative fines for any infringement of this Regulation, in addition to, or instead of any other appropriate measures pursuant to this Regulation. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. For the purpose of setting a fine under this Regulation, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 of the Treaty. ***It should not be permitted to impose double penalties resulting from***

the violation of both Regulation (EU) 2016/279 and this Regulation.

Or. fr

Amendment 131
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Article 1 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.	1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data ***regardless of whether a payment is required by the user***.

Or. en

Amendment 132
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 1 – paragraph 2

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

Or. en

Amendment 133
Daniel Buda

Proposal for a regulation
Article 1 – paragraph 3

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

Or. ro

Amendment 134
Max Andersson

Proposal for a regulation
Article 1 – paragraph 3

Text proposed by the Commission	*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.	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. ***Except where otherwise provided for in this Regulation, the provisions of Regulation (EU) 2016/679 shall apply when personal data is processed.***

Or. en

Amendment 135
Mady Delvaux

Proposal for a regulation
Article 1 – paragraph 3

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

Or. en

Amendment 136
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 1 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Where the specific rules in paragraph 3 involve processing of personal data that are subject to Regulation (EU) 2016/679, both Regulations apply. In cases of conflict between the two Regulations, the European Data Protection Board shall determine the instrument that should apply.

Or. en

Amendment 137
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 1 – paragraph 3 b (new)

Text proposed by the Commission	*Amendment*
	3b. When making a determination in line with paragraph 4, the European Data Protection Board shall consider that the interests for natural persons are paramount.

Or. en

Amendment 138
Jiří Maštálka, Kateřina Konečná

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 in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users ***regardless of whether a payment is required by the user***.

Or. en

Amendment 139
Daniel Buda

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

Or. ro

Amendment 140
Mady Delvaux

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 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.

Or. en

Amendment 141
Max Andersson

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***:***

Or. en

Amendment 142
Max Andersson

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 from the end-user is required.

Or. en

Amendment 143
Max Andersson

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.

Or. en

Amendment 144
Max Andersson

Proposal for a regulation
Article 2 – paragraph 1 – point c (new)

Text proposed by the Commission	*Amendment*
	(c) the placing on the market of hardware and software permitting electronic communications by end-users, including the retrieval and presentation of information on the Internet;

Or. en

Amendment 145
Max Andersson

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 communication;

Or. en

Amendment 146
Max Andersson

Proposal for a regulation
Article 2 – paragraph 1 – point e (new)

Text proposed by the Commission	*Amendment*
	(e) the sending of commercial electronic communications concerning direct marketing to end-users.

Or. en

Amendment 147
Max Andersson

Proposal for a regulation
Article 2 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) electronic communications services which are not publicly available;	***deleted***

Or. en

Amendment 148
Max Andersson

Proposal for a regulation
Article 2 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;	(d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security***, without prejudice to article 11***;

Or. en

Amendment 149
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 2 – paragraph 2 – point d a (new)

Text proposed by the Commission	*Amendment*
	(da) hardware and software placed on the market permitting electronic communications between users or end-users, including the presentation of information on the Internet

Or. en

Amendment 150
Max Andersson

Proposal for a regulation
Article 2 – paragraph 3

Text proposed by the Commission	*Amendment*
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].	3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies ***insofar as they are not publicly available and not originating or having as destination publicly available communications services,*** is governed by

Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001].

Or. en

Amendment 151
Max Andersson

Proposal for a regulation
Article 3 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. This Regulation applies to:	1. This Regulation applies to ***the activities referred to in Article 2 where the user or end-user is in the Union or where the communications services, hardware, software, directories, or direct marketing commercial electronic communications are provided from the territory of the Union.***
(a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;	
(b) the use of such services;	
(c) the protection of information related to the terminal equipment of end-users located in the Union.	

Or. en

Amendment 152
Mady Delvaux

Proposal for a regulation
Article 3 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) the protection of information related to the terminal equipment of end-users ***located*** in the Union.	(c) the protection of information related to ***or processed by*** the terminal equipment of end-users in the Union.

Or. en

Amendment 153
Jens Rohde

Proposal for a regulation
Article 3 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) the protection of information related to the terminal equipment of end-users ***located*** in the Union.	(c) the protection of information related to the terminal equipment of end-users in the Union.

Or. en

Justification

The territorial scope should include all end-users in the Union

Amendment 154
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 3 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) the protection of information related to the terminal equipment of end-users ***located*** in the Union.	(c) the protection of information related to the terminal equipment of end-users in the Union.

Or. en

Amendment 155
Mady Delvaux

Proposal for a regulation
Article 3 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Where the provider of an electronic	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.	communications service***, provider of a publicly available directory, software provider enabling electronic communications or person sending direct marketing commercial communications or collecting (other) information related to or stored in the end-users terminal equipment*** is not established in the Union it shall designate in writing a representative in the Union.

Or. en

Amendment 156
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 3 – paragraph 4

Text proposed by the Commission	*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, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.	4. The representative shall ***be authorised by the provider*** to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, ***courts*** and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation ***and shall be provided with any relevant information to that end by the provider, to the extent that the provider does not answer the questions or provide the information directly***.

Or. en

Amendment 157
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Article 3 – paragraph 4

Text proposed by the Commission	*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, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.	4. The representative shall ***be authorised by the provider*** to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, ***courts*** and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation ***and shall be provided with any relevant information to that end by the provider, to the extent that the provider does not answer the questions or provide the information directly***.

Or. en

Amendment 158
Max Andersson

Proposal for a regulation
Article 3 – paragraph 4

Text proposed by the Commission	*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, and end-users, on all issues related ***to processing electronic communications data*** for the purposes of ensuring compliance with this Regulation.	4. The representative shall 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 ***the activities referred to in Article 2*** for the purposes of ensuring compliance with this Regulation.

Or. en

Amendment 159
Max Andersson

Proposal for a regulation
Article 3 – paragraph 5

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

Or. en

Amendment 160
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 3 a (new)

Text proposed by the Commission	*Amendment*
	Article 3a
	Applicable law in the online environment
	1. To the extent that Regulation (EU) 2016/679 or this Regulation allow Member States to regulate the processing of personal data or electronic communications data, in their domestic laws, the relevant national law provisions shall apply to:
	(a) the processing of personal data or electronic communications data in the context of the activities of an establishment of a controller, processor or a provider of an electronic communications service or network established in the Member State in question; or
	(b) the processing of personal data or electronic communications data by a controller, processor or a provider of an electronic communications service or network not established in the Union ,

offering goods or services in that Member State or monitoring the behaviour of data subjects in that Member State;

2. The relevant national law provisions as set out in point 1 of this Article do not apply to the processing of personal data or electronic communications data in the context of the activities of an establishment of a controller, processor or a provider of an electronic communications service or network established in another Member State, who shall instead only be subject to the relevant national law provisions of that other Member State.

Or. en

Amendment 161
Jiří Maštálka, Kateřina Konečná, Kostas

Proposal for a directive
Article 4 – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(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]***;	(b) ‘electronic communications ***newtwork***’ ***means transmission systems, whether or not based on a permanent infrastructure or centralized 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;

Or. en

Amendment 162
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 4 – paragraph 1 – point b a (new)

Text proposed by the Commission	*Amendment*
	(ba) 'user or end-user' means a natural person using a publicly available electronic communications service, without necessarily having subscribed to this service;

Or. en

Amendment 163
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 4 – paragraph 1 – point b b (new)

Text proposed by the Commission	*Amendment*
	(bb) 'number-based interpersonal communications service' means an interpersonal communications service which uses assigned numbering resources, i.e. a number or numbers in national or international telephone numbering plans partly or fully as its addressing system;

Or. en

Amendment 164
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 4 – paragraph 1 – point b c (new)

Text proposed by the Commission	*Amendment*
	(bc) 'call' means a connection established by means of a publicly available electronic interpersonal communications service allowing voice communication between two or more endpoints;

Or. en

Amendment 165
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 4 – paragraph 1 – point b d (new)

Text proposed by the Commission	*Amendment*
	(bd) 'electronic communication service' means service normally provided for remuneration via electronic communications networks, which encompasses 'internet access service' as defined in Article 2(2) of Regulation (EU) 2015/2120; and/or 'interpersonal communications service'; and/or services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;

Or. en

Amendment 166
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 4 – paragraph 1 – point b e (new)

Text proposed by the Commission	*Amendment*
	(be) 'interpersonal communications service' means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks. This includes services that enable interpersonal and interactive communication as a minor ancillary feature that is intrinsically linked to another service;

Or. en

Amendment 167
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

Proposal for a regulation
Article 4 – paragraph 1 – point b f (new)

Text proposed by the Commission	*Amendment*
	(bf) '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;

Or. en

Amendment 168
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

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

Text proposed by the Commission	*Amendment*
	(aa) 'normally for remuneration' means involving an economic transaction, whether financial or not;

Or. en

Amendment 169
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

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 exchanged by means of electronic communications services ***or via electronic communications networks*** , such as text, voice, videos, images, and sound;

Or. en

Amendment 170
Isabella Adinolfi, Marco Zullo

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 exchanged by means of electronic communications services ***or via electronic communications networks***, such as text, voice, videos, images, and sound;

Or. en

Amendment 171
Isabella Adinolfi, Marco Zullo

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

Text proposed by the Commission	*Amendment*
(c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;	(c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including***, but not limited to,*** data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication; ***It includes data broadcast or emitted by the terminal equipment to identify end-users' communications and/or terminal equipment in the network and enable it to connect to such network or to another device.***

Or. en

Amendment 172
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

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	(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

services, and the date, time, duration and the type of communication;	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.***

Or. en

Amendment 173
Axel Voss

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

Text proposed by the Commission	*Amendment*
(f) 'direct marketing communications' means any form of ***advertising***, whether written or oral, sent ***to one or more*** identified or identifiable end-users of ***electronic*** communications ***services***, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;	(f) 'direct marketing communications' means any form of ***communication for the purpose of promoting products and services***, whether written or oral, sent ***directly to an*** identified or identifiable end-users of ***an interpersonal*** communications ***service***, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc. ***For the purposes of this regulation, an interpersonal communications service shall also include a service that is not provided for remuneration***;

Or. en

Amendment 174
Isabella Adinolfi, Marco Zullo

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

Text proposed by the Commission	*Amendment*
(f) 'direct marketing communications'	(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.;	means any form of advertising ***or similar promotion, sent, directed or presented*** to one or more identified or identifiable end-users ***over an*** of electronic communications ***network***, including the use of automated calling and communication systems with or without human interaction, ***targeted advertising on social media platforms,*** electronic mail***, facsimile***, SMS, etc.;

Or. en

Amendment 175
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

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

Text proposed by the Commission	*Amendment*
(f) 'direct marketing communications' means any form of advertising***, whether written or oral, sent*** to one or more identified or identifiable end-users ***of*** electronic communications ***services***, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;	(f) 'direct marketing communications' means any form of advertising ***or similar promotion sent, directed or presented*** to one or more identified or identifiable end-users ***over an*** electronic communications ***network***, including the use of automated calling and communication systems with or without human interaction, ***targeted advertising on social media platforms,*** electronic mail***, facsimile***, SMS, etc.;

Or. en

Amendment 176
Jean-Marie Cavada

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

Text proposed by the Commission	*Amendment*
(f) 'direct marketing communications' means any form of ***advertising***, whether written or oral, sent to one or more	(f) 'direct marketing communications' means any form of ***commercial communication***, whether written or oral,

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.;	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.;

Or. fr

Amendment 177
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

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

Text proposed by the Commission	*Amendment*
(g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems;	(g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems; ***and which connect the caller and the recipient of the call with or without the use of semi-automated communication systems, such as for example automatic dialers***;

Or. en

Amendment 178
Jiří Maštálka, Kateřina Konečná, Kostas Chrysogonos

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

Text proposed by the Commission	*Amendment*
	(ha) 'new equipment location data' means data that can enable the geospatial location, movement or direction of terminal equipment and is not processed in order to provide a communications service;

Or. en

Amendment 179
Isabella Adinolfi, Marco Zullo

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

Text proposed by the Commission	*Amendment*
	(ha) 'equipment location data' means data that can enable the geospatial location, movement or direction of terminal equipment and is not processed in order to provide a communications service;

Or. en

Amendment 180
Max Andersson

Proposal for a regulation
Chapter 2 – title

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

Or. en

Amendment 181
Daniel Buda

Proposal for a regulation
Article 5 – title

Text proposed by the Commission	*Amendment*
Confidentiality of electronic communications ***data***	Confidentiality of electronic communications ***content***

Or. ro

Amendment 182
Max Andersson

Proposal for a regulation
Article 5 – title

Text proposed by the Commission	*Amendment*
Confidentiality of electronic communications ***data***	Confidentiality of electronic communications

Or. en

Amendment 183
Max Andersson

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission	*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 or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	***deleted***

Or. en

Amendment 184
Angel Dzhambazki

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission	*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 ***or processing*** of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	Electronic communications data shall be confidential. Any interference with electronic communications data ***during conveyance***, such as by ***unauthorized*** 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. ***The processing of electronic communications data following conveyance to the intended recipients or their service provider shall be subject to Regulation (EU) 2016/679.***

Or. en

Amendment 185
Jens Rohde

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission	*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 or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	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. ***The provisions of Regulation (EU) 2016/679 shall apply unless this Regulation stipulates special provisions.***

Or. en

Amendment 186
Isabella Adinolfi, Marco Zullo

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission	*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 or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	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.

Or. en

Amendment 187
Daniel Buda

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission	*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 or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	Electronic communications data shall be confidential. Any interference with electronic communications data ***during conveyance***, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications content, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.

Or. ro

Amendment 188
Mady Delvaux

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission	*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 or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	Electronic communications data shall be confidential. Any interference with electronic communications data, ***at rest or in transit,*** such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or ***any*** processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.

Or. en

Amendment 189
Max Andersson

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

Text proposed by the Commission	*Amendment*
	Electronic communications data shall be confidential. Any processing of electronic communications data, including 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, 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.

Or. en

Amendment 190
Axel Voss

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

Text proposed by the Commission	*Amendment*
	For the implementation of paragraph 1, providers of electronic communications networks and services shall take technical and organisational measures as defined in Article 32 of Regulation (EU) 2016/679. Additionally, to protect the integrity of terminal equipment and the safety, security and privacy of users, providers or electronic communications networks and services shall take appropriate measures based on the risk and on the state of the art to reasonably prevent the distribution through their networks or services of malicious software as referred to in Article 7 subparagraph a of Directive 2013/40/EU.

Or. en

Amendment 191
Isabella Adinolfi, Marco Zullo

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

Text proposed by the Commission	*Amendment*
	Neither providers of electronic communication services nor any third parties shall process electronic communications data that are not collected on the basis of consent or any other legal ground under this Regulation, or any other legal basis not specifically provided for in this Regulation.

Or. en

Amendment 192
Max Andersson

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

Text proposed by the Commission	*Amendment*
	Confidentiality of electronic communications shall also apply to data related to or processed by terminal equipment and to machine-to-machine communication.

Or. en

Amendment 193
Mady Delvaux

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

Text proposed by the Commission	*Amendment*
	Confidentiality of electronic communications data shall also include terminal equipment and machine-to-machine communications when related to a user.

Or. en