European Parliament
2014-2019

Committee on the Internal Market and Consumer Protection

2017/0003(COD)

3.7.2017

AMENDMENTS
44 - 180

Draft opinion
Eva Maydell
(PE604.857v01-00)

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 44
Jan Philipp Albrecht

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

Or. en

Amendment 45
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Liisa Jaakonsaari, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

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, e-mail, internet phone calls***, in-platform messages between users of a*** social ***network and any private messaging systems online***.

Or. en

Amendment 46
Daniel Dalton, Richard Sulík

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***	(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These

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***.

metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing conclusions to be drawn regarding the private lives of the persons involved in the electronic communication.

Or. en

Amendment 47
Inese Vaidere

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

activities of everyday life, their interests, tastes etc.

Or. en

Amendment 48
Curzio Maltese

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 activities of everyday life, their interests, tastes etc.	(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. ***These data includes text, voice, videos, images, sounds, the IP and MAC addresses of end-users,*** 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.

Or. en

Justification

In principle, content and metadata should benefit from the same level of protection. It has been shown many times that metadata give as much relevant information as content linked to end-users private life (see: https://techcrunch.com/2016/05/17/stanford-quantifies-the-privacy-stripping-power-of-metadata/ or https://www.privacyinternational.org/node/53). There is no justification anymore to make a difference on the level of protection for metadata and content.

Amendment 49
Jan Philipp Albrecht

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 activities of everyday life, their interests, tastes etc.	(2) Electronic communications ***data*** may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc. ***The protection of confidentiality of communications is an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, freedom of assembly, freedom of expression and information.***

Or. en

Justification

This amendment serves to underline the importance of this particular piece of legislation.

Amendment 50

Daniel Dalton, Richard Sulík

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.	***deleted***

_____

[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 51

Anna Maria Corazza Bildt

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.	***deleted***

_____

[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

Inese Vaidere

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. Therefore, the provisions of this Regulation should apply to both natural and legal persons ***in addition to rules provided in Directive 2016/943/EU***. 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.
[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 53

Jan Philipp Albrecht

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. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that ***certain*** provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council[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 54
Jan Philipp Albrecht

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data ***may include*** personal data as defined in Regulation (EU) 2016/679.	(4) Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data ***are generally*** personal data as defined in Regulation (EU) 2016/679***, at least where the users or end-users are natural persons***.

Or. en

Amendment 55
Curzio Maltese

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data may include personal data as defined in Regulation (EU) 2016/679.	(4) Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data may include ***and, as regards natural persons, are always*** personal data as defined in Regulation (EU) 2016/679.

Or. en

Justification

Clarifies which electronic communications data are personal data.

Amendment 56
Jan Philipp Albrecht

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

Or. en

Justification

This clarification is encouraged by the European Data Protection Supervisor.

Amendment 57
Daniel Dalton, Richard Sulík

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 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 ***and do not go beyond or contradict the high level of protection set down in Regulation (EU) 2016/679***. 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.

Or. en

Amendment 58
Curzio Maltese

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 by providers of electronic communications services should only be permitted in accordance with this Regulation. ***Where both this Regulation and the Regulation (EU) 2016/679 may apply to the same processing, this Regulation only should apply.***

Or. en

Justification

Clarifies how the two Regulations will apply together.

Amendment 59
Inese Vaidere

Proposal for a regulation
Recital 6

Text proposed by the Commission	*Amendment*
(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[22] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an ***inconsistent or insufficient effective protection*** of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of online behaviour of end-users, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.	(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[22] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an ***insufficient clarity and inconsistent enforcement*** 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).	[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 60
Jan Philipp Albrecht

Proposal for a regulation
Recital 6

Text proposed by the Commission	*Amendment*
(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[22] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of ***online behaviour of*** end-users, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.	(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council[22] remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. 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 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. en

Amendment 61
Jan Philipp Albrecht

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

Justification

This recital would undermine the approach of harmonisation of the Digital Single Market by means of a Regulation.

Amendment 62
Kaja Kallas, Dita Charanzová

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	(7) The ***European Data Protection Board*** should***, where necessary, issue guidance and opinions*** within the limits of this Regulation to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. ***Cooperation and consistency between Member States, in particular between national data protection***

protection of private life and personal data and the free movement of electronic communications data.	***authorities, is essential to*** maintain a balance between the protection of private life and personal data and the free movement of electronic communications data ***in the Union***.

Or. en

Amendment 63
Curzio Maltese

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) 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, Member States should ***introduce provisions increasing end-users' privacy without compromising*** the free movement of electronic communications.

Or. en

Amendment 64
Christel Schaldemose, Lucy Anderson, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

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

Or. en

Amendment 65
Anna Maria Corazza Bildt

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 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 persons who use electronic communications services to send direct marketing commercial communications or collect information related to or stored in ***consumers***' terminal equipment.

Or. en

Amendment 66
Jan Philipp Albrecht

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

Or. en

Justification

Alignment with the General Data Protection Regulation.

Amendment 67
Curzio Maltese

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 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 ***or use the processing capabilities of such terminal equipment***.

Or. en

Justification

Limiting how the processing capabilities of the terminal equipment of end-users may be used should be clearly included in the broad scope of this Regulation. This recital is not clear on this point as it stands.

Amendment 68
Inese Vaidere

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 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 ***make*** direct marketing commercial communications or collect information related to or stored in end-users' terminal equipment.

Or. en

Amendment 69
Jan Philipp Albrecht

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	(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.	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

Justification

Alignment with the General Data Protection Regulation.

Amendment 70
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Liisa Jaakonsaari, Kerstin Westphal, Marc Tarabella, Josef Weidenholzer

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 71
Jan Philipp Albrecht

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. ***This Regulation aims at ensuring*** an effective and equal protection of end-users when using functionally equivalent services, ***so as to ensure the confidentiality of their communication, irrespective*** of the ***technological medium chosen***. 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; 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)).

Or. en

Amendment 72
Eva Maydell

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***	(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.

that are ancillary to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.

---

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

---

[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 73
Sabine Verheyen

Proposal for a regulation
Recital 12

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

2014/53/EU.

Or. de

Amendment 74
Daniel Dalton, Richard Sulík

Proposal for a regulation
Recital 12

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

Or. en

Amendment 75
Eva Maydell, Antonio López-Istúriz White, Antanas Guoga

Proposal for a regulation
Recital 12

Text proposed by the Commission	*Amendment*
(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.	(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU. ***Regulation shall not apply to machine-to-machine communications which are not provided as a service targeting the general public. Moreover, the provision of machine-to-machine platforms shall not be considered to be an electronic communications service solely by the inclusion of service other than the mere conveyance of communication data (such as collecting and making machine-to-machine data available to end-users via (i) the platform, (ii) offering functions to analyse the machine-to-machine data via the platform or (iii) transfer signals to operate and control the machines via the platform).***

Or. en

Amendment 76
Jan Philipp Albrecht

Proposal for a regulation
Recital 12

Text proposed by the Commission	*Amendment*
(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.	(12) Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. ***In the context of automated supply-chains and elsewhere in the manufacturing or industrial context, the communication by the machines involved may not be inter-personal and may not involve natural persons. However, its confidentiality still needs protection in order to protect internal business information.*** Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.

Or. en

Amendment 77
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as ***'hotspots'*** situated at different places within a city, department stores, shopping ***malls*** and hospitals. To the extent that those communications networks are provided to ***an undefined group of end-users***, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of ***the corporation***.	(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as ***Wi-Fi access points*** situated at different places within a city, ***for example*** department stores, shopping ***centres*** and hospitals***, as well as airports, public transport, hotels and restaurants. Those Wi-Fi access points might require a login or a password and might be provided also by public administrations***. To the extent that those communications networks are provided to ***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 ***addition, this Regulation should apply to closed social media profiles and groups that the user has restricted or defined as private. In*** contrast, this Regulation should not apply to closed groups of end-users such as corporate ***intranet*** networks, access to which is limited to members of ***an organisation***.

Or. en

Amendment 78
Jan Philipp Albrecht

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as ***'hotspots'*** situated at different places within a city, department stores, shopping malls ***and hospitals***. To the extent that those communications networks are provided to ***an undefined group of end-users***, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, ***access*** to which is limited to members of the ***corporation***.	(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as ***wireless internet access points*** situated at different places within a city, department stores, shopping malls***, hospitals, airports, hotels and restaurants. Those access points might require a login or provide a password and might be provided also by public administrations, including Union bodies and agencies***. To the extent that those communications networks are provided to ***users***, the confidentiality of the communications transmitted through such networks should be protected. 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. ***This regulation should also apply to closed social media profiles and groups that the users have defined as private.*** In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, to which ***access*** is limited to members of the ***organisation***.

Or. en

Amendment 79
Daniel Dalton, Richard Sulík

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. ***The fact that wireless*** electronic communications services ***may be ancillary to other*** services should not ***stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast,*** this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.	(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls 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. ***This Regulation should apply to electronic communications data using publically available*** electronic communications services ***and public communications networks. In this context, publicly available means only*** services ***intended for consumers. It*** should not ***include services intended for business users, nor should the means of the delivery of the service in question, whether obtained over the public internet or not have any bearing on the interpretation of whether the service is publicly available or not.*** 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 80
Curzio Maltese

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of	(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of

internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to ***an undefined group of*** end-users, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and ***public*** communications networks***. In contrast, this Regulation should not apply to closed groups of end-users such as corporate*** networks***, access to which is limited to members of the corporation***.	internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to 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 communications networks***, irrespective of whether these services and*** networks ***are publicly available or not***.

Or. en

Justification

Services not publicly available are excluded from the scope of telecommunications regulations for reasons specific to such regulations (for instance, it would be unjustified to impose access obligations on networks not publicly available). However, this distinction is irrelevant as regards the confidentiality of communications: all communications should be protected equally, irrespective of end-users' location. Therefore, electronic communications services which are not publicly available should remain within the scope of this regulation.

Otherwise, excluding them from this scope would allow companies to monitor how their employees are using their access to the network, which is unacceptable: companies only need to assess the work done by their employees, not to monitor each of their actions.

Amendment 81
Kaja Kallas, Dita Charanzová

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.	(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation. ***The mere act of requiring a password should not be considered as providing access to a closed group of end-users if the access is provided to an undefined group of end-users.***

Or. en

Amendment 82
Daniel Dalton, Richard Sulík

Proposal for a regulation
Recital 14

Text proposed by the Commission	*Amendment*
(14) Electronic communications 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. 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.

should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting electronic communications content.

Or. en

Amendment 83
Jan Philipp Albrecht

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	(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged

(electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.

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

Or. en

Amendment 84
Curzio Maltese

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 subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.	(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. 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 ***from the perspective of Internet access providers*** and therefore be subject to the provisions of this Regulation***. Data generated, processed or transmitted by interpersonal communications services for the purpose of sending, transmitting or receiving such communications should be considered as electronic communications metadata from the perspective of the providers of these services but should still be considered as electronic communications content from the perspective of Internet access***

providers. 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

Justification

The definition of metadata depends on which layer of the network is considered. On layer 3 (“transmission” - See the OSI model https://en.wikipedia.org/wiki/OSI_model), the metadata and the content processed by OTT on higher level (“application” and “content”) are all transmitted together in TCP/IP packets. Telecommunications operators make no distinction between the metadata and the content processed by OTT. From the perspective of operators, these data are the “content” transmitted on the network.

This recital should make this technical clarification.

Amendment 85
Jan Philipp Albrecht

Proposal for a regulation
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) Modern electronic communications services, including the internet and the services that run on top of it, function on the basis of the separation of layers of protocols and services, as defined by the Open Systems Interconnection model (OSI model, ISO/IEC 7498-1). An internet (TCP/IP) data packet for example is encapsulated in an underlying ethernet or wireless data packet for local routing. One layer above, an e-mail including its content and metadata is encapsulated in one or more TCP/IP packets. The e-mail, in turn, consists of metadata using the SMTP protocol, and content data in the body of the e-mail. That means that what is

metadata on one protocol layer is normally content data for the layers below. Where this Regulation lays down different rules for the processing of content and metadata, this should be understood for the respective electronic communications service and the protocol layer it is operating on. An internet access provider, for example, should therefore not scan the content of the TCP/IP packets routed by it, in order to detect malicious e-mail senders or attachments, because for the internet layer, e-mail is fully content. The scanning of e-mails however could be done by the e-mail provider if it is necessary for security of the service or if the user specifically requests this.

Or. en

Justification

This explains the clarification added in the definitions of "content" and "metadata" in Article 4.

Amendment 86
Jan Philipp Albrecht

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***	(15) Electronic communications data should be treated as confidential. This means that any ***processing of electronic communications data or any*** interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. ***When the processing is allowed under this Regulation, any other***

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.

processing on the basis of Article 6 of Regulation (EU) 2016/679 should be considered as prohibited, including processing for another purpose on the basis of Article 6(4) of that Regulation. This should not prevent requesting additional consent for new processing operations. The prohibition of ***processing*** of communications data should apply during their conveyance ***and when they are stored afterwards, in order to reflect the growing trend that end-users do not store all communications data on their own terminal equipment, but use cloud-based storage space of the communications provider or other parties***. 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 ***other*** parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the ***user*** concerned. As technology evolves, the technical ways to 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 customers' traffic data,*** including browsing habits***,*** without the ***users***' consent.

Or. en

Amendment 87
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Josef Weidenholzer

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	(15) Electronic communications should be treated as confidential. This means that any interference with the transmission of electronic communications, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. ***When the processing is allowed under any exception to the prohibitions under this Regulation, any other processing on the basis of Article 6 of Regulation (EU) 2016/679 should be considered as prohibited, including processing for another purpose on the basis of Article 6(4) of that Regulation. This should not prevent requesting additional consent for new processing operations.*** The prohibition of interception of communications should apply ***also*** during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee***, and to 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 ***other*** parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the ***user*** concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation

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

Amendment 88
Curzio Maltese

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***	(15) Electronic communications data should be treated as confidential. This means that any interference with 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. ***Interfering means to process electronic*** communications data ***for any purpose not requested by all end-users concerned, whether such process is carried out before, during or after the transmission of communications. Interference with*** 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.

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.	***Interference*** 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 ***interference*** 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 ***interference*** include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.

Or. en

Justification

As it stands, this recital may limit the scope of article 5 to interferences which only occurs during the transmission of communications. This would prevent communications data from being protected before and after the transmission. Thus, this recital needs clarification.

Amendment 89
Jan Philipp Albrecht

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	(16) The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission. It should not prohibit either the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including

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.	checking security threats ***related to the respective service,*** or the processing of metadata ***of the respective service*** to ensure the necessary quality of service requirements, such as latency, jitter etc.

Or. en

Amendment 90
Eva Maydell, Antonio López-Istúriz White, Antanas Guoga, Roberta Metsola

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. ***The processing of anonymous data by providers, and making data anonymous, should be incentivised as the act of anonymization dramatically reduces the risk from a privacy and security perspective associated with processing of data related to transmission. This Regulation also*** should not prohibit either the processing of electronic communications data to ensure the security***, confidentiality, integrity, availability, authenticity*** and continuity of the electronic communications services ***and networks***, including checking security threats 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 91
Daniel Dalton, Richard Sulík

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 in the electronic communications network. ***The processing of pseudonymised data, should be incentivized as the act of psedonymisation dramatically reduces any privacy and security risk associated with processing of data related to transmission.*** 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 ***appropriate*** quality of service requirements, such as latency, jitter etc.

Or. en

Amendment 92
Sabine Verheyen

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	(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

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.	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. de

Amendment 93
Eva Maydell, Pascal Arimont, Antanas Guoga, Anna Maria Corazza Bildt

Proposal for a regulation
Recital 16 a (new)

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

Or. en

Amendment 94
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Josef Weidenholzer

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. 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.

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 95
Curzio Maltese

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	(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. 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, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Where a type of processing of electronic communications metadata, in particular using new technologies, and

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.

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

Justification

Location data are highly sensitive data especially as they enable one of the highest form of surveillance. They shall benefit from the higher level of protection.

Amendment 96
Jan Philipp Albrecht

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***	(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. 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. 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 ***may be*** necessary to link the positions of individuals at certain time intervals. 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 processing of electronic communications ***data is foreseen***, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority

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.

should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.

Or. en

Amendment 97
Daniel Dalton, Richard Sulík

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	(17) The processing of electronic communications ***metadata*** can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, ***in accordance with Article 6(1) and 6(4) of Regulation (EU) No 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

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.

communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to ***comply with Regulation (EU) No 2016/679 when processing*** electronic communications metadata, which should include data on the location of the device***.*** ***As an exception from obtaining end-users' consent, the processing of electronic communications metadata for purposes other than those for which the personal data were initially collected should be allowed in cases where further processing is compatible in accordance with Article 6(4) of Regulation (EU) 2016/679.*** 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***. Therefore, whenever the purpose(s) of further processing cannot be achieved by processing data that is made anonymous, pseudonymisation of data should be allowed***. 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 98
Sabine Verheyen

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	(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 ***in accordance with 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 ***comply with Regulation (EU) 2016/679 when processing*** 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

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.***	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.

Or. de

Amendment 99
Andreas Schwab

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 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

(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 ***in accordance with 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 ***comply with Regulation (EU) 2016/679 when processing*** 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.	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. de

Amendment 100
Jan Philipp Albrecht

Proposal for a regulation
Recital 17 a (new)

Text proposed by the Commission	*Amendment*
	(17a) This Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata based on users' informed consent. However, users attach great importance to the confidentiality of their communications, including their online activities, and they want to control the use of their electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to obtain users' consent to process electronic communications data. For the purposes of this Regulation, the consent of a user should have the same meaning and be subject to the same conditions as the consent of the data subject under Regulation (EU) 2016/679.
	Or. en

Amendment 101
Jan Philipp Albrecht

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 ***electronic communications data*** to receive specific services ***requested by them, such as protection*** services against ***malware, unsolicited communication, or fraudulent activities***. ***Consent for processing electronic communications data will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment. As provided by Article 7 of*** Regulation (EU) 2016/679***, consent is not freely given if it is required to access any service or obtained through insistent and repetitive requests. In order to prevent such abusive requests, end-users should be able to order service providers to remember their*** choice ***not to*** consent.

Or. en

Amendment 102
Curzio Maltese

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 ***data*** to receive specific services. 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. ***Consent for processing data will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment. As provided by article 7*** of the ***Regulation (EU) 2016/679,*** consent ***is not freely given if it is required to access any service or obtained through insisting and repetitive requests. In order to prevent such abusive requests, users shall be able to order service providers to remember their choice not to consent***.

Or. en

Justification

Consent should be freely given for any kind of processing. The GDPR is not making any distinction between processing. This Regulation should not do this either.

Furthermore, end-users shall be protected from harassing requests leading to consent fatigue and to unfreely given consent.

Amendment 103
Inese Vaidere

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 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. ***The end-user must be informed about the possible further use of their personal data by third parties.*** 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.

Or. en

Amendment 104
Curzio Maltese

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	(19) Electronic communications ***data*** pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under

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.

Article 7 of the Charter. Any interference with electronic communications ***data*** 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 ***electronic communications data***, this Regulation sets forth a presumption that the processing of such 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. After electronic communications ***data*** has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679. ***Where communications data are stored by a third party, this third party should encrypt from end to end any information which processing is not necessary to provide the service requested by the end-user.***

Or. en

Justification

Content and metadata should benefit from the same level of protection.

Providers shall encrypt from end to end communications where technically feasible.

Amendment 105
Jan Philipp Albrecht

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 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***	(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any ***processing of*** content ***data*** of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility ***for*** 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 ***electronic*** communications ***data***, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always ***carry out an impact assessment as provided for in*** Regulation (EU) 2016/679 ***and if necessary under that Regulation, consult the supervisory authority prior to the*** processing. After electronic 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 ***another*** party entrusted by them to record or store such data***, which***

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.

could be the electronic communications provider. Any processing of such ***stored communications data where the data is stored on behalf of the end-user must comply with this Regulation. The end-user may further process the data, and if it contains personal data,*** must comply with Regulation (EU) 2016/679.

Or. en

Amendment 106
Kaja Kallas, Dita Charanzová

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 persons. When processing such type of data, the provider of the electronic communications service should always	(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. ***For services that are provided to users engaged in purely personal or household activities, the consent of the end-user requesting the service should be sufficient.*** Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high

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. en

Amendment 107
Jan Philipp Albrecht

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 specifically requested by a user for personal or personal work-related purposes such as search or keyword indexing functionality, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools by persons with disabilities. This should be possible without the consent of all users who are

part of the communication, but may take place with the consent of the user requesting the service. Such specific consent also precludes the provider from processing those data for different purposes.

Or. en

Amendment 108
Jan Philipp Albrecht

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	(20) Terminal equipment of ***users*** of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the ***users*** requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes ***very sensitive data*** that may reveal details of ***the behaviour, psychological features,*** emotional ***condition and*** political ***convictions, religious beliefs and*** social complexities ***of an individual***, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information ***processed by or*** related to such equipment requires enhanced privacy protection. ***Information related to the user's device may also be collected remotely for the purpose of***

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.

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

Or. en

Amendment 109
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Kerstin Westphal, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

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

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

Amendment 110

Sabine Verheyen

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 ***and*** hidden identifiers 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 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 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. de

Amendment 111
Inese Vaidere

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	(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.

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. ***End-users refusal to give consent for placing tracking tools on their terminal equipment cannot be a ground for refusing to give access to content, if an operation of the service or during a provision of the service it is not necessary.***

Or. en

Amendment 112
Anna Maria Corazza Bildt

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***	(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***. For

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.

instance, the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a service requested by the ***consumer***. This may include the storing of cookies for the duration of a single established session on a website to keep track of the ***consumer'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 or their exploitation 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 ***consumer's*** settings and the mere logging of the fact that the ***consumer's*** device is unable to receive content requested by the ***consumer*** should not constitute access to such a device or use of the device processing capabilities.

Or. en

Amendment 113
Jan Philipp Albrecht

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

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

information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for 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 ***user***. This may include the storing of ***information (such as*** cookies ***and identifiers)*** for the duration of a single established session on a website to keep track of the ***end-user's*** input when filling in online forms over several pages. Information society ***service*** providers that engage in configuration checking to provide the service in compliance with the ***user's*** settings and the mere logging of the fact that the user's device is unable to receive content requested by the ***user*** should not constitute ***illegitimate access***.

Or. en

Amendment 114
Curzio Maltese

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	(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in ***or emitted by*** 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

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.	authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of ***remembering the choice of end-users not to give their consent to other processing or for the 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. 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. en

Amendment 115
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

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	(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***.

user. This may include the storing of ***information (such as*** cookies ***and identifiers)*** for the duration of a single established session on a website to keep track of the user's input when filling in online forms over several pages. ***Tracking techniques, if implemented with appropriate privacy safeguards,*** can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers ***could*** engage in configuration checking ***in order*** to provide the service in compliance with the ***user's*** settings and the mere logging ***revealing*** the fact that the user's device is unable to receive content requested by the ***user,*** should not constitute ***illegitimate access***.

Or. en

Amendment 116
Eva Maydell, Antanas Guoga

Proposal for a regulation
Recital 21

Text proposed by the Commission	*Amendment*
(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in	(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in

online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

online forms over several pages. ***Consent should also not be necessary if the information processed or stored is necessary to protect privacy, security or safety of the end-user, or to protect confidentiality, integrity, availability and authenticity of the terminal equipment.*** 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. As an exemption from obtaining end-user´s consent, the processing of information and data that are or are rendered pseudonymous or anonymous should be allowed or for purposes other than those for which they were initially collected in cases where the processing is compatible and is subject to specific safeguards, especially pseudonymisation as set forth in point (4) of Article 6 of Regulation (EU) 2016/679***

Or. en

Amendment 117
Daniel Dalton, Richard Sulík

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	(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.

privacy. For instance, consent should not be requested for authorizing the technical storage or access which is 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 personalisation 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 requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

Or. en

Amendment 118
Daniel Dalton, Richard Sulík

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	(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***.	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 appropriate ***technical*** settings.

Or. en

Amendment 119
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Liisa Jaakonsaari, Marc Tarabella, Josef Weidenholzer

Proposal for a regulation
Recital 22

Text proposed by the Commission	*Amendment*
(22) The methods used for providing information and obtaining end-user's	(22) The methods used for providing information and obtaining end-user's

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

consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, ***users*** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, ***users*** are overloaded with requests to provide consent. 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. In this sense, settings must be granular enough to control all data processing that the user consents to and to cover all relevant functionalities (for example, whether websites or apps can collect location data from the user or can access specific hardware such as a webcam or microphone). Devices and software applications enabling electronic communications should implement technical mechanisms such as the Do Not Track standard to ensure that users' privacy is protected by default and that users are given genuine choice and control.***

Or. en

Amendment 120
Jan Philipp Albrecht

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***	(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, ***users*** are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, ***users*** are overloaded with requests to provide consent. ***This Regulation should prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.*** The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent ***and to object by technical specifications*** using ***automated means, such as*** the appropriate settings of a ***hardware of software permitting the retrieval and presentation of information on the internet. Those settings should include choices concerning the use of processing and storage capabilities of the user's terminal equipment as well as a signal sent by the hardware or software indicating the user's preferences to*** other ***parties***. The choices made by ***users*** when establishing its general privacy settings of a ***hardware of software*** should be binding on, and enforceable against, any third parties. Web

helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

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. ***More particularly*** web browsers***, applications or mobile operating systems may be used as a user's personal privacy assistant communicating the user's choices, thus helping end-users to prevent information related to or processed by their terminal equipment (for example smart phone, tablet or computer) from being accessed, processed or stored. They should therefore not abuse their position as gate-keepers and still allow for possibilities for the user to individually give consent with regard to a certain specific service or service provider***.

Or. en

Amendment 121
Curzio Maltese

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	(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 ***but their choice not to consent is rarely remembered by service providers***. As a result, end-users are overloaded with requests to provide consent. ***Imposing specific and limited obligations on service providers*** may address this problem.

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.	Therefore, this Regulation should provide for the possibility ***for end-users to order service providers to remember their choice not to consent and to stop requesting their consent once they have refused to give it. The choices made by end-users*** application should be binding on, and enforceable against, any third parties. ***Furthermore,*** 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.

Or. en

Justification

Consent is not freely given if end-users who had already refused to give it may be requested to do so over and over again, impeding their use of the service, until they finally give it.

Amendment 122
Kaja Kallas, Dita Charanzová

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	(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***.	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, ***unauthorised*** 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. ***On the other hand, in light of the pace of innovation, the increasing use and range of devices that permit communications and the increase of cross-device tracking, it is necessary for this Regulation to remain technology neutral to meet its objectives***.

Or. en

Amendment 123
Eva Maydell, Antanas Guoga

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 from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.	(22) The methods used for providing information and obtaining end-user's consent should be 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***, provided that there is no separate specific consent given by the end-user***. Web browsers are a type of software application that permits the retrieval and presentation of information on 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.

Or. en

Amendment 124
Andreas Schwab

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 from their terminal equipment (for example	(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.	smart phone, tablet or computer) from being accessed or stored. ***Steps should be taken, however, to ensure that this gatekeeper function is not misused.***

Or. de

Amendment 125
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Kerstin Westphal, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

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 ***are*** codified under Article 25 of Regulation (EU) 2016/679. ***Hardware manufacturers and providers of software permitting electronic communications should have an obligation to configure devices and software so that their default settings provide the highest level of privacy protection possible, protecting users' against cross-domain tracking and unauthorised interferences with their communications and terminal equipment. Users should be informed about the default privacy settings and any available options to change those settings during installation or first use of the device or software and when they make significant changes to it.*** Privacy ***settings should be presented in an objective, easily visible and intelligible manner. They should be easily accessible and modifiable during the use of the device or software. Information provided should not incentivise users to select lower*** privacy settings ***and*** should ***include relevant information about the risks associated with each setting***.

Or. en

Amendment 126
Daniel Dalton, Richard Sulík

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. ***Therefore providers of software enabling publically available electronic communications services and permitting*** the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers end-users a set of privacy setting options ***in order that end-users may actively select a preferred option after being given the necessary information to make the choice***. Such privacy settings should be presented in *an* easily visible and intelligible manner.

Or. en

Amendment 127
Pascal Arimont

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.	(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.

Providers of software enabling electronic communication, including the retrieval and presentation of information on the internet, should have an obligation to ***pre-set*** the software ***in such a way as to offer end-users the highest level of protection of their privacy and, in particular,*** prevent third parties from storing information on the terminal equipment; End-users may be offered a set of privacy setting options, ranging from ***intermediate to lower protection***. Such privacy settings should ***come with a warning about the risks associated with lowering the level of protection and*** be presented in a an easily visible and intelligible manner.

Or. de

Amendment 128
Anna Maria Corazza Bildt

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***	(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. ***Therefore providers of software enabling publicly available electronic communications services and permitting*** 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***. Consumers*** should be offered a set of privacy setting options. Such privacy settings should be presented in an easily visible and intelligible manner.

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.

Or. en

Amendment 129
Eva Maydell, Antanas Guoga

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 ***inform the end-user about the possibility to express his or her consent using appropriate technical settings. The end-user should be offered multiple options to choose from, including*** to prevent third parties from storing information on the terminal equipment. End-users should be offered a set of privacy setting options, ranging from***, for example, rejecting tracking that is not necessary for the functionality of the website or other software to,*** for example, ***accepting tracking necessary for the functionality of the website or other software as well as for other purposes or,*** for example, ***accepting tracking necessary for the functionality of the website or other software and tracking for other purposes by parties that demonstrate the compliance with the EU data protection and privacy legislation, for instance in***

line with Article 40 and 42 of Regulation (EU) 2016/679. Such privacy settings should be presented in an easily visible and intelligible manner.

Or. en

Amendment 130
Kaja Kallas

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 ***for end-users to choose whether to reject or to accept cookies that are not necessary for the provision of the service requested by the end-user, after being informed of the function of the*** cookies***, how they are used, and how the information gathered is shared***. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate ***options according to the types of information they are willing to share, the parties they agree to share it with, the purposes of a cookie, and the possibility to opt out from cross-device tracking. Where the end-user accepts*** cookies ***for purpose of targeted advertising, the end-user should also be able to correct the information gathered about him or her to prevent the possible harm caused by inaccurate information***.

Privacy settings should be presented in *an* easily visible and intelligible manner.

Or. en

Amendment 131
Jan Philipp Albrecht

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 ***hardware or*** software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers ***and activates as default*** the option to prevent ***the cross-domain tracking and*** storing information on the terminal equipment ***by other parties***; this is often presented as 'reject third party ***trackers and*** cookies'. ***Users*** should be offered a set of privacy setting options, ranging from higher (for example, 'never accept ***trackers and*** cookies') to lower (for example, 'always accept ***trackers and*** cookies') and intermediate (for example, 'reject ***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 and, among other aspects, reflect the possibility that another*** party ***might act as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service. 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 and intelligible manner***, and users should be informed about the possibility to change the default privacy settings among the various options at the moment of installation or first use. Information provided should not dissuade users from selecting higher privacy settings and should include relevant information about the risks associated to allowing cross-domain trackers, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising or sharing with more third parties. Hardware and software manufacturers should be required to provide easy ways for users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain information society services or to specify for such services websites trackers and cookies are always or never allowed. In case of no active choice, or action from the user, the settings shall be set by default in a manner that rejects and blocks trackers, including cookies, that are not strictly necessary in order to provide an information society service specifically requested by the user***.

Or. en

Amendment 132
Curzio Maltese

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'***, which prevents end-users from providing informed and freely given consent, overloading them with requests***. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers ***and sets by default*** the option to prevent third parties from ***requesting end-users' consent to store*** 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 ***ask whether to*** accept cookies ***but always reject them***') to lower (for example, 'always ***ask whether to*** accept cookies') and intermediate (for example, 'reject third party cookies ***without asking***' or 'only ***ask whether to*** accept first party ***cookies and reject other*** cookies'). Such privacy settings should be presented in *an* easily visible and intelligible manner.

Or. en

Justification

End-users should not be able to express their consent through automated means (for example through technical settings of a software application enabling access to the internet) but, in order not to be overloaded with requests, they should be able to automatically reject some categories of request.

Amendment 133
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Liisa Jaakonsaari, Kerstin Westphal, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

Proposal for a regulation
Recital 23 a (new)

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

Or. en

Amendment 134
Kaja Kallas

Proposal for a regulation
Recital 23 a (new)

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

Or. en

Amendment 135
Curzio Maltese

Proposal for a regulation
Recital 24

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

Or. en

Justification

Consent expressed through automated means (for example through technical settings of a software application enabling access to the internet) can never be informed nor valid.

Amendment 136
Jan Philipp Albrecht

Proposal for a regulation
Recital 24

Text proposed by the Commission	*Amendment*
(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged	***deleted***

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

Justification

Integrated into Recital 23 for greater clarity.

Amendment 137
Daniel Dalton, Richard Sulík

Proposal for a regulation
Recital 24

Text proposed by the Commission	*Amendment*
(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade	***deleted***

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 138
Anna Maria Corazza Bildt

Proposal for a regulation
Recital 24

Text proposed by the Commission	*Amendment*
(24) For ***web browsers*** to be able to obtain ***end-users***' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the ***end-user*** of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if ***end-users*** are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation,	(24) For ***software enabling publicly available communication services and permitting the retrieval and presentation of information on the internet*** to be able to obtain ***consumers***' 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 ***consumer using*** 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 ***consumers*** are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary

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***.

information to make the choice. To this end, it is necessary to require providers of software enabling access to internet ***in the context of publicly available electronic communications services*** that, at the moment of installation, ***consumers*** 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 ***consumers*** from selecting higher privacy settings***. Such obligations do not arise where the software already seeks to prevent*** third ***parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment***. Web browsers are encouraged to provide easy ways for ***consumers*** to change the privacy settings at any time during use.

Or. en

Amendment 139
Kaja Kallas

Proposal for a regulation
Recital 24

Text proposed by the Commission	*Amendment*
(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of ***third party tracking cookies***, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select ***'accept third party cookies'*** to confirm their agreement and are given the	(24) For web browsers ***or other applications*** to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of ***tracking cookies that are not necessary for the provision of a specific service requested by an end user***, 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

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***.

are required to actively select ***cookies that process data beyond what is necessary for the service to function*** to confirm their agreement and are given the necessary information to make the choice. ***Consent should not be valid for cross-device tracking if the end-user was not informed and is not able to opt out.*** To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing ***certain*** 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 ***or other applications*** 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 ***parties or cookies that are always or never allowed. In cases where a business model is based on targeted advertising, consent should not be considered as freely given if the access to the service is made conditional to data processing. The end-user should therefore be able to choose between accepting cookies or being provided the service in exchange for payment***.

Or. en

Amendment 140
Pascal Arimont

Proposal for a regulation
Recital 24

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

Amendment 141
Inese Vaidere

Proposal for a regulation
Recital 24

Text proposed by the Commission	*Amendment*
(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.	(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 ***or present*** 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 142
Curzio Maltese

Proposal for a regulation
Recital 25

Text proposed by the Commission	*Amendment*
(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to end-users, for example when they enter stores, with 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***	(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. ***In any case, being able to precisely locate individuals is one of the highest form of surveillance. It should never occur without end-users' consent. Furthermore, service providers should not even be allowed to use information emitted by terminal equipment in order to request such consent, otherwise they would be able to harass end-users for their consent and***

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***.

prevent them from providing freely given ***consent. Instead, providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users that they may contact them, or download a specific application on their terminal equipment, in order to be properly informed about the intended processing and to provide their consent***.

Or. en

Justification

Tracking end-users' device should only be authorised if end-users actively consent to be tracked. Such a consent would not be freely given if providers may be able to automatically send numerous requests to all end-users entering the monitored area.

Amendment 143
Christel Schaldemose, Lucy Anderson, Liisa Jaakonsaari, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

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	(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.

who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to ***users***, for example when they enter stores, with personalized offers. While some of these functionalities ***may*** not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. ***Users' privacy should be adequately protected in these situations. Information emitted by terminal equipment of users when connecting to a network or other device should only be processed should only be allowed for specific and transparent purposes if the users have consented or if the processing is necessary for statistical counting, as long as such counting is carried out for public utility purposes, there are no other means to achieve the envisaged purpose and that the measures established in Article 35 and*** Article ***36*** of Regulation (EU) 2016/679 ***have been fulfilled***.

Or. en

Amendment 144
Anna Maria Corazza Bildt

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	(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.

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 ***consumers***, for example when they enter stores, with personalized offers. ***Information emitted by terminal equipment should be considered a separate category from metadata and information from the consumer's terminal equipment itself. Nevertheless, collection of such information should be subject to specific transparency measures and safeguards. Entities deploying such solutions*** should display ***or make available*** prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679 ***and the processing of such personal data will also be subject to the Regulation***.

Or. en

Amendment 145
Jan Philipp Albrecht

Proposal for a regulation
Recital 25

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

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***.

process such electronic communications metadata based on the consent of the ***users concerned***.

Or. en

Amendment 146
Kaja Kallas, Dita Charanzová

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	(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***.

specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should ***ask for the consent*** of the ***end-users concerned, or where consent is not possible, such practices should be limited to what is strictly necessary for*** the purpose of ***statistical counting, be limited in time and space and the data made anonymous or erased as soon as it is no longer needed for this purpose***.

Or. en

Amendment 147
Eva Maydell, Antonio López-Istúriz White, Antanas Guoga

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	(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.

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 ***ask for the end-user´s consent or should carry out data protection impact assessment and in this case the data collected is or is rendered pseudonymous or anonymous. Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, prior consultation with the supervisory authority, as prescribed in Article 36 of Regulation (EU) 2016/679, should be carried out. Providers should*** display 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 148
Jan Philipp Albrecht

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	(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction ***is targeted at persons suspected of having committed a criminal offence and*** constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should ***not be obliged by Union or Member States*** competent authorities ***to weaken any measures that ensure the integrity and confidentiality of electronic communications***.

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)***.

Or. en

Amendment 149
Curzio Maltese

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	(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 the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above ***the fight against serious crimes and if such measures cannot be taken without the prior authorisation of a court*** , in accordance with the Charter of Fundamental Rights of the European Union and the European

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).

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).

Or. en

Amendment 150
Kaja Kallas

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***	(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. Therefore, this Regulation should not affect the ability

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).

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).

Or. en

Amendment 151
Kaja Kallas

Proposal for a regulation
Recital 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by

design. Member States should not impose any obligation on encryption providers, on providers of electronic communications services or on any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of "backdoors".

Or. en

Amendment 152
Anna Maria Corazza Bildt, Eva Maydell

Proposal for a regulation
Recital 27

Text proposed by the Commission	*Amendment*
(27) As regards calling line identification, it is necessary to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. ***Certain end-users, in particular help lines, and similar organisations, have an interest in guaranteeing the anonymity of their callers.*** As regards connected line identification, it is necessary to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected.	(27) As regards calling line identification, it is necessary to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. As regards connected line identification, it is necessary to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected. ***These requirements make sense in the context of two-way voice communication services conducted on a one-to-one basis. They do not make sense, and are not technically feasible, in the context of other publicly available interpersonal communication services such as SMS text applications, or multi-party and multimedia communication platforms, enabling concurrent communications in the form of voice, video, messaging and document sharing for multiple participants. Given there are multiple parties involved it is not possible for each of them to exercise the***

right to prevent caller identification without impinging on the rights of the other parties for such identification not to be suppressed.

Or. en

Amendment 153
Anna Maria Corazza Bildt, Eva Maydell

Proposal for a regulation
Recital 28

Text proposed by the Commission	*Amendment*
(28) There is justification for overriding the elimination of calling line identification presentation in specific cases. ***End-users***' rights to privacy with regard to calling line identification should be restricted where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services, such as eCall, to carry out their tasks as effectively as possible.	(28) There is justification for overriding the elimination of calling line identification presentation in specific cases. ***Consumers***' rights to privacy with regard to calling line identification should be restricted where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services, such as eCall, to carry out their tasks as effectively as possible.

Or. en

Amendment 154
Anna Maria Corazza Bildt, Eva Maydell

Proposal for a regulation
Recital 29

Text proposed by the Commission	*Amendment*
(29) Technology exists that enables providers of electronic communications services to limit the reception of unwanted calls by ***end-users*** in different ways, including blocking silent calls and other fraudulent and nuisance calls. Providers of publicly available ***number-based***	(29) Technology exists that enables providers of ***certain publicly available*** electronic communications services to limit the reception of unwanted calls by ***consumers*** in different ways, including blocking silent calls and other fraudulent and nuisance calls. ***Where technically***

interpersonal communications services should deploy this technology and protect ***end-users*** against nuisance calls and free of charge. Providers should ensure that ***end-users*** are aware of the existence of such functionalities, for instance, by publicising the fact on their webpage.

feasible and economically viable, providers of publicly available ***voice*** communications services should deploy this technology and protect ***consumers*** against nuisance calls and free of charge. Providers should ensure that ***consumers*** are aware of the existence of such functionalities, for instance, by publicising the fact on their webpage.

Or. en

Amendment 155
Jan Philipp Albrecht

Proposal for a regulation
Recital 29

Text proposed by the Commission	*Amendment*
(29) Technology exists that enables providers of electronic communications services to limit the reception of unwanted calls by end-users in different ways, including blocking silent calls and other fraudulent and nuisance calls. Providers of publicly available number-based interpersonal communications services should deploy this technology and protect end-users against nuisance calls and free of charge. Providers should ensure that end-users are aware of the existence of such functionalities, for instance, by publicising the fact on their webpage.	(29) Technology exists that enables providers of electronic communications services to limit the reception of unwanted calls by end-users in different ways, including blocking silent calls and other fraudulent and nuisance calls ***or marketing calls with a specific code or prefix***. Providers of publicly available number-based interpersonal communications services should deploy this technology and protect end-users against nuisance calls and ***do so*** free of charge. Providers should ensure that end-users are aware of the existence of such functionalities, for instance, by publicising the fact on their webpage.

Or. en

Amendment 156
Daniel Dalton, Richard Sulík

Proposal for a regulation
Recital 30

Text proposed by the Commission	*Amendment*
(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person requires that end-users that are natural persons are ***asked for consent before their personal data are*** included in ***a*** directory. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.	(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person ***acting out of their business capacity*** requires that end-users that are natural persons are ***provided, upon request, with transparent information about the data being*** included in ***the*** directory ***and the means to verify, correct, update, supplement and delete data relating to them free of charge***. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.

Or. en

Amendment 157
Morten Løkkegaard, Gérard Deprez, Jean-Marie Cavada, Fredrick Federley, Pavel Telička

Proposal for a regulation
Recital 30

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

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

Or. en

Justification

The publicly available directories are now based on a functional opt-out system. This proposal would create an opt-in system, where the providers are forced to gain consent from all end-users, creating an unnecessary burden for the providers. Securing the end-user's right to object should be sufficient.

Amendment 158
Eva Maydell, Antanas Guoga

Proposal for a regulation
Recital 30

Text proposed by the Commission	*Amendment*
(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person requires that end-users that are natural persons are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory.	(30) Publicly available directories of end-users of electronic communications services are widely distributed. Publicly available directories means any directory or service containing end-users information such as phone numbers (including mobile phone numbers), email address contact details and includes inquiry services. The right to privacy and to protection of the personal data of a natural person requires that end-users that are natural persons are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory. ***The consent should be collected by the electronic communications service provider at the moment of signing the contract for such***

service.

Or. en

Amendment 159
Daniel Dalton, Richard Sulík

Proposal for a regulation
Recital 31

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

Or. en

Amendment 160
Morten Løkkegaard, Gérard Deprez, Jean-Marie Cavada, Fredrick Federley, Pavel Telička

Proposal for a regulation
Recital 31

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

Or. en

Justification

The publicly available directories are now based on a functional opt-out system. This proposal would create an opt-in system, where the providers are forced to gain consent from all end-users, creating an unnecessary burden for the providers. Securing the end-user's right to object should be sufficient.

Amendment 161
Jan Philipp Albrecht

Proposal for a regulation
Recital 31

Text proposed by the Commission	*Amendment*
(31) If end-users that are natural persons give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in	(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.	the directory (for example name, email address, home address, user name, phone number). In addition, providers of publicly available directories ***or the providers of electronic communications services*** should inform the end-users of the purposes of the directory and of the search functions of the directory 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.

Or. en

Amendment 162
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Marc Tarabella, Arndt Kohn, Josef Weidenholzer

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 ***or presents*** direct marketing communications directly to one or more identified or identifiable ***users*** using electronic communications services***, regardless of the form that such marketing takes***. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.

Or. en

Amendment 163
Anna Maria Corazza Bildt, Eva Maydell

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 ***consumers*** 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.

Or. en

Amendment 164
Inese Vaidere

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	(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends***, presents or makes*** 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

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.

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.

Or. en

Amendment 165
Anna Maria Corazza Bildt, Eva Maydell

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 of rules that do not vary according to the technology used to convey these unsolicited communications, while at the	(33) Safeguards should be provided to protect ***consumers*** against unsolicited communications for direct marketing purposes, which intrude into the private life of ***consumers***. 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 ***consumers*** is obtained before commercial electronic communications for direct marketing purposes are sent to ***consumers*** in order to effectively protect individuals against the intrusion into their private life. 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

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.

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.

Or. en

Amendment 166
Jan Philipp Albrecht

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***, including*** for direct marketing purposes. 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 ***end-users that are*** 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

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.

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.

Or. en

Amendment 167
Eva Maydell, Pascal Arimont

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	(33) Safeguards should be provided to protect end-users against unsolicited communications for direct marketing purposes, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, emails, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons. Legal certainty and the need to ensure that

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

Or. en

Amendment 168
Pascal Arimont

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	(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.

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

Or. de

Amendment 169
Anna Maria Corazza Bildt

Proposal for a regulation
Recital 34

Text proposed by the Commission	*Amendment*
(34) When ***end-users*** have provided their consent to receiving unsolicited communications for direct marketing purposes, they should still be able to withdraw their consent at any time in an easy manner. To facilitate effective enforcement of Union rules on unsolicited messages for direct marketing, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes. Unsolicited marketing communications should therefore be clearly recognizable as such	(34) When ***consumers*** have provided their consent to receiving unsolicited communications for direct marketing purposes, they should still be able to withdraw their consent at any time in an easy manner. To facilitate effective enforcement of Union rules on unsolicited messages for direct marketing, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes. Unsolicited marketing communications should therefore be clearly recognizable as such

and should indicate the identity of the legal or the natural person transmitting the communication or on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to oppose to receiving further written and/or oral marketing messages.	and should indicate the identity of the legal or the natural person transmitting the communication or on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to oppose to receiving further written and/or oral marketing messages.

Or. en

Amendment 170
Anna Maria Corazza Bildt

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 code identifying the fact that the call is a marketing call.	(35) In order to allow easy withdrawal of consent, natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by ***consumers*** to withdraw their consent. Natural persons conducting direct marketing communications through ***voice-to-voice*** calls and through calls by automating calling and communication systems should display their identity line on which the company can be called or present a specific code identifying the fact that the call is a marketing call.

Or. en

Amendment 171
Pascal Arimont

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 code identifying the fact that the call is a marketing call.	(35) In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called ***and*** present a specific code identifying the fact that the call is a marketing call.

Or. de

Amendment 172
Inese Vaidere

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 ***caller*** 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.

Or. en

Amendment 173
Kaja Kallas, Dita Charanzová

Proposal for a regulation
Recital 37

Text proposed by the Commission	*Amendment*
(37) ***Service providers who offer electronic communications services should inform end- users of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security risks does not discharge a*** service ***provider from the*** obligation to ***take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level*** of the ***service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679***.	(37) ***The*** service ***providers are under*** obligation to ***provide services that are secure and notify security breaches in accordance with Regulation (EU) 2016/679, [Directive*** of the ***European Parliament and of the Council establishing the European Electronic Communications Code] and Directive (EU) 2016/1148***.

Or. en

Amendment 174
Jan Philipp Albrecht

Proposal for a regulation
Recital 37

Text proposed by the Commission	*Amendment*
(37) Service providers who offer electronic communications services should ***inform end- users*** of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about	(37) Service providers who offer electronic communications services should ***process electronic communications data in such a way as to prevent unauthorised processing, including access, disclosure or alteration. They should ensure that such unauthorised access, disclosure or alteration is possible of being ascertained, and also ensure that electronic communications data are protected by using state of the art software and encryption technologies. Service providers should also inform end-users*** of measures they can take to protect ***their anonymity***

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

Or. en

Amendment 175
Christel Schaldemose, Lucy Anderson, Olga Sehnalová, Marc Tarabella, Josef Weidenholzer

Proposal for a regulation
Recital 39

Text proposed by the Commission	*Amendment*
(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.	(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks set forth in this Regulation. In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have the same tasks and effective powers in each Member State, without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. ***Supervisory authorities should cooperate with the***

relevant authorities in other enforcement areas as appropriate.

Or. en

Amendment 176
Inese Vaidere

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. ***The fines imposed should not lead to irreversible consequences to the undertaking in case insignificant 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.

Or. en

Amendment 177
Eva Maydell, Antanas Guoga, Roberta Metsola

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. ***Double penalties resulting from the infringement of both this Regulation and Regulation (EU) 2016/679 should be avoided.***

Or. en

Amendment 178
Kaja Kallas, Dita Charanzová

Proposal for a regulation
Recital 41

Text proposed by the Commission	*Amendment*
(41) ***In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[25] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore,*** in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.	(41) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

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

Or. en

Amendment 179
Jan Philipp Albrecht

Proposal for a regulation
Recital 43

Text proposed by the Commission	*Amendment*
(43) Directive 2002/58/EC should be repealed.	(43) Directive 2002/58/EC ***and Commission Regulation (EU) 611/2013*** should be repealed.

Or. en

Justification

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

Amendment 180
Roberta Metsola

Proposal for a regulation
Recital 43 a (new)

Text proposed by the Commission	*Amendment*
	(43a) The successful functioning of innovative future network infrastructure such as Fifth Generation (5G) networks is dependent on an increasing number of devices, often with limited computational capacity, being able to process data at unprecedented speeds. The end-user's

privacy in such a scenario remains a priority and should therefore be designed to complement the requirements of such infrastructure and allow free movement of the electronic communication data for 5G to operate as intended and satisfy the needs of end-users, operators, industry verticals, businesses and law and policymakers.

Or. en