

**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (Text with EEA relevance)**

2017/0003(COD)

DRAFT [4 column tabled E privacy regulation - rev 4 May 2021]

05-05-2021 at 14h18

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Formula				
1	2017/0003 (COD)	2017/0003 (COD)	2017/0003 (COD)	
Proposal Title				
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (Text with EEA relevance)	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (Text with EEA relevance)	
Formula				
3	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Citation 1				
4	Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,	
Citation 2				
5	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	
Citation 3				
6	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	
Citation 4				
7	Having regard to the opinion of the European Economic and Social Committee <sup>1</sup> ,  1. OJ C , , p. .	Having regard to the opinion of the European Economic and Social Committee <sup>1</sup> ,  1. OJ C , , p. .	Having regard to the opinion of the European Economic and Social Committee <sup>1</sup> ,  1. OJ C , , p. .	
Citation 5				
8	Having regard to the opinion of the	Having regard to the opinion of the	Having regard to the opinion of the	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	Committee of the Regions <sup>1</sup> , <u>1. OJ C , , p. .</u>	Committee of the Regions <sup>1</sup> , <u>1. OJ C , , p. .</u>	Committee of the Regions <sup>1</sup> , <u>1. OJ C , , p. .</u>	
Citation 6				
9	Having regard to the opinion of the European Data Protection Supervisor <sup>1</sup> , <u>1. OJ C , , p. .</u>	Having regard to the opinion of the European Data Protection Supervisor <sup>1</sup> , <u>1. OJ C , , p. .</u>	Having regard to the opinion of the European Data Protection Supervisor <sup>1</sup> , <u>1. OJ C , , p. .</u>	
Citation 7				
10	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	
Formula				
11	Whereas:	Whereas:	Whereas:	
Recital 1				
12	(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.	(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.	(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 <del>privacy</del> confidentiality of one's communications is an essential	(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	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 <del>parties involved in a communication</del> <b>communicating parties</b> . 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 <del>personal</del> <b>inter-personal</b> messaging provided through social media. <i><b>It should also apply when the confidentiality of electronic communications and the privacy of the physical environment converge, i.e. where terminal devices for electronic communications can also listen into their physical environment or use other input channels such as Bluetooth signalling or movement sensors.</b></i>  AM 1	dimension of this right, <b>applying both to natural and legal persons</b> . 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.	(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.
Recital 2				
13	(2) The content of electronic	(2) The content of electronic	(2) The content of electronic	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	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. <b><i>Metadata can also be processed and analysed much easier than content, as it is already brought into a structured and standardised format. The protection of confidentiality of communications is an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and</i></b>	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 <del>includes</del> <b>include</b> 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.	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>religion, freedom of assembly, freedom of expression and information.</i>  AM 2		
Recital 2a				
13a			<b>(2a) Regulation (EU) 2016/679 regulates the protection of personal data. This Regulation protects in addition the respect for private life and communications. The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid 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. The provisions particularise Regulation (EU) 2016/679 as regards personal data by translating its principles into specific rules. If no specific rules are established in this Regulation, Regulation (EU) 2016/679 should apply to any processing of data that qualify as personal data. The provisions complement Regulation (EU) 2016/679 by setting forth rules regarding subject matters</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			that are not within the scope of Regulation (EU) 2016/679, such as the protection of the rights of end-users who are legal persons. Processing of electronic communications data by providers of electronic communications services and networks should only be permitted in accordance with this Regulation. This Regulation does not impose any obligations on the end-user End-users who are legal persons may have rights conferred by Regulation (EU) 2016/679 to the extent specifically required by this Regulation	
Recital 3				
14	(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 <sup>1</sup> , also apply to end-users who are legal persons. This includes the definition of consent under		(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value <b>and the protection of which allows legal persons to conduct their business, supporting among other innovation.</b> Therefore, the provisions of this Regulation should <b>in principle</b> apply to both natural and legal persons. Furthermore, this Regulation should ensure that, <b>where necessary</b> , provisions of the Regulation (EU) 2016/679 of the	(17) For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p> <p>1. 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).</p>		<p>European Parliament and of the Council<sup>111</sup>, also apply <b>mutatis mutandis</b> to end-users who are legal persons. This includes the <b>provisions on definition of consent</b> under Regulation (EU) 2016/679. <del>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.</del></p> <p>1. 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).</p>	
Recital 3a				
14a			<p><b>(3a) This Regulation should not affect national law regulating for instance the conclusion or the validity of a contract. Similarly, this Regulation should not affect</b></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<b>national law in relation to determining who has the legal power to represent legal persons in any dealings with third parties or in legal proceedings.</b>	
Recital 4				
15	(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 <del>may include</del> <b>are generally</b> personal data as defined in Regulation (EU) 2016/679.  AM 3	(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.	(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.
Recital 5				
16	(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	(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	Deleted	(10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms,

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	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. <del>Processing of electronic communications data by providers</del> <b>On the contrary, it aims to provide additional and complementary safeguards take into account the need for additional protection as regards the confidentiality of communications. Processing</b> of electronic communications <del>services</del> <b>data</b> should only be permitted in accordance with this Regulation.  AM 4		which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.  (21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.
Recital 6				
17	(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council <sup>1</sup> 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	(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council <sup>1</sup> 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	(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council <sup>1</sup> 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	(4) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(5) translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector.

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p> <p>1. 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).</p>	<p>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 <del>online behaviour of end-users, which are not covered by Directive 2002/58/EC</del> users. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.</p> <p>1. 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):</p> <p>AM 5</p>	<p>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.</p> <p>1. 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).</p>	<p>Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.</p>
Recital 7				
18	<p>(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</p>	<p>(7) The <del>Member States</del> <b>European Data Protection Board</b> should, <b>where necessary, issue guidance and opinions</b> <del>be allowed</del>, within the limits of this Regulation, to maintain or introduce national provisions to</p>	<p>(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</p>	<p>(48) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. <del>Therefore, the margin of discretion, which Member States have in this regard, should</del> <b>Cooperation and consistency between Member States, in particular between national Data Protection Authorities, is essential to</b> maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.  AM 6	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.	composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.
Recital 7a				
18a			<b>(7a) This Regulation does not apply to the protection of fundamental rights and freedoms related to activities which fall outside the scope of Union law, and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those operations, whether it is a public authority or a private operator acting at the request of a public</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			authority.	
Recital 8				
19	(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 <i>transmitted to, stored in</i> , related to or <del>stored in end-users</del> <i>processed by users</i> ' terminal equipment. <a href="#">AM 7</a>	(8) This Regulation should apply to providers of electronic communications services, <b>and</b> to providers of publicly available directories, <del>and to software providers permitting electronic communications, including the retrieval and presentation of information on the internet.</del> This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing commercial communications or <b>make use of processing and storage capabilities of terminal equipment</b> or collect information <del>related to</del> <b>processed by or emitted by</b> or stored in end-users' terminal equipment.	
Recital 8a				
19a			<b>(8a) Furthermore, this Regulation should apply regardless of whether the processing of electronic communications data or personal data of end-users who are in the Union takes place in the Union or not, or of whether the</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>service provider or person processing such data is established or located in the Union or not.</p> <p>Former 8aaa</p>	
Recital 8b				
19b			<p>(8b) Some end-users, for example providers of payment services or payment systems, process as recipients their electronic communications data for different purposes or request a third party to process their electronic communications data on their behalf. It is also important that end-users, including legal entities, have the possibility to take the necessary measures to secure their services, networks, employees and customers from security threats or incidents. Information security services may play an important role in ensuring the security of end-users' digital sphere. For example, an end-user as an information society service provider may process its electronic communications data, or may request a third party, such as a provider of security technologies and services, to process that end-user's electronic communications</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>data on its behalf, for purposes such as ensuring network and information security, including the prevention, monitoring and termination of fraud, unauthorised access and Distributed Denial of Service attacks, or facilitating efficient delivery of website content. Processing of their electronic communications data by the end-users concerned, or by a third party entrusted by the end-users concerned to process their electronic communications data after receipt on their behalf, should not be covered by this Regulation. For the purpose of protecting the end-user's terminal equipment processing upon receipt, including also just before receipt, by a third party entrusted should not be covered by this Regulation.</p> <p>Former 8aa</p>	
Recital 8c				
19c			<p>(8c) This Regulation does not apply to the electronic communications data of deceased persons. Member States may provide for rules regarding the</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			processing of electronic communications data of deceased persons.  Former 8a	
Recital 9				
20	(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 <del>provision</del> <b>offering</b> 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. <b><i>This should be the case irrespective of whether the electronic communications are connected to a payment or not. For the purpose of this Regulation, where the provider of an electronic communications service is not established in the Union, it should designate, in writing, a representative in the Union.</i></b>  AM 8	Deleted	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Recital 10				
21	<p>(10) Radio equipment and its software which is placed on the internal market in the Union, must comply with Directive 2014/53/EU of the European Parliament and of the Council<sup>1</sup>. This Regulation should not affect the applicability of any of the requirements of Directive 2014/53/EU nor the power of the Commission to adopt delegated acts pursuant to Directive 2014/53/EU requiring that specific categories or classes of radio equipment incorporate safeguards to ensure that personal data and privacy of end-users are protected.</p> <p><sup>1</sup> Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).</p>		<p>(10) Radio equipment and its software which is placed on the internal market in the Union, must comply with Directive 2014/53/EU of the European Parliament and of the Council<sup>1</sup>. This Regulation should not affect the applicability of any of the requirements of Directive 2014/53/EU nor the power of the Commission to adopt delegated acts pursuant to Directive 2014/53/EU requiring that specific categories or classes of radio equipment incorporate safeguards to ensure that personal data and privacy of end-users are protected.</p> <p><sup>1</sup> Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).</p>	
Recital 11				
22	<p>(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-</p>	<p>(11) The services used for communications purposes, and the technical means of their delivery,</p>	<p>(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-</p>	<p>(5) New advanced digital technologies are currently being introduced in public communications networks in the</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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<sup>1</sup>]. 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.</p>	<p>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, <b>also known as "over-the-top-services" (OTTs). This Regulation aims at ensuring- In order to ensure</b> an effective and equal protection of end-users when using functionally equivalent services, <del>this Regulation uses the definition of electronicso as to</del> <b>ensure the confidentiality of their</b> communications, <b>irrespective services set forth in the [Directive of the European Parliament and of the Council establishing the European Electronic Communications Code<sup>1</sup>]- That definition encompasses technological medium chosen. It does</b> not only cover internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. <del>The protection of confidentiality of</del> <b>communications is crucial also as</b></p>	<p>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<sup>1</sup>}(EU) <b>2018/1972<sup>1</sup></b>. 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. <del>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.</del></p>	<p>Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.</p> <p>(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.</p> <p>(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	1. 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)).	<del>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.</del>  <del>1. 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)).</del>  AM 9	1. <b>Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).</b> 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)).	freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.
Recital 11a				
22a			<b>(11a) The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, the processing of electronic communications data in the context of the provision of such type of minor ancillary services should be covered by this Regulation.</b>	
Recital 11b				
22b			<b>(11b) In all the circumstances</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>where electronic communication is taking place between a finite, that is to say not potentially unlimited, number of end-users which is determined by the sender of the communications, e.g. any messaging application allowing two or more people to connect and communicate, such services constitute interpersonal communications services. Conversely, a communications channel does not constitute an interpersonal communications service when it does not enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s). This is for example the case when the entity providing the communications channel is at the same time a communicating party, such as a company that operates a communications channel for customer care that allows customers solely to communicate with the company in question. Also, where access to an electronic communications is available for anyone, e.g.</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			communications in an electronic communications channel in online games which is open to all persons playing the game, such channel does not constitute an interpersonal communications feature. This reflects the end-users' expectations regarding the confidentiality of a service.  Former 11aa	
Recital 12				
23	(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	<del>(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</del>	<del>(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.</del> <b>The use of machine-to-machine and Internet of Things services, that is to say services involving an automated transfer of data and information between devices or software-based applications with limited or no human interaction, is emerging.</b> In order to ensure full protection of the rights to privacy and confidentiality	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	<del>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.</del> AM 10 deleted	of communications, and to promote a trusted and secure Internet of Things in the digital single market, <del>it is necessary to clarify that this Regulation</del> <b>this Regulation, in particular the requirements relating to the confidentiality of communications, should apply to the transmission of such services. The transmission of machine-to-machine or Internet of Things services regularly involves the conveyance of signals via an electronic communications network and, hence, constitutes an electronic communications service. This Regulation should apply to the provider of the transmission service if that transmission is carried out via a publicly available electronic communications service or network. Conversely, Therefore, where the transmission of machine-to-machine or Internet of Things services is carried out via a private or closed network such as a closed factory network, the principle of confidentiality enshrined in this Regulation should also not apply. Typically, providers of machine-to-machine or Internet of Things services operate at the application layer (on top of electronic to the transmission of machine to machine</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			communications services). These service providers and their customers who use IoT services are in this respect end-users, and not providers of the electronic communication service and therefore benefit from the protection of confidentiality of their electronic communications data. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.	
Recital 13				
24	(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	(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 <del>hotspots</del> <b>wireless internet access points</b> situated at different places within a city, <b>for example</b> department stores, shopping malls <del>and</del> , hospitals. <del>To the extent that, airports, hotels and restaurants. Those communications networks are provided to an undefined group of end-users, the confidentiality of the communications transmitted through such networks should be protected.</del>	(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, <b>regardless if these networks are secured with passwords or not</b> , the confidentiality of the communications transmitted through such networks should be protected.	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	<del>The fact that wireless electronic access points might require a log in or provide a password and might be provided also by public administrations, including Union bodies and agencies. To the extent that those communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of</del> <b>networks are provided to users, the confidentiality of the communications data and application of this Regulation transmitted through such networks should be protected.</b> Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. <b>This Regulation should also apply to closed social media profiles and groups that the users have restricted or defined as private.</b> In contrast, this Regulation should not apply to closed groups of end-users such as corporate <i>intranet</i> networks, access to which is limited to members of <i>an organisation</i> . <b>The mere requirement of a password should not be considered as providing access to a closed group of end-users if the access to the</b>	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 <b>publicly available</b> electronic communications services and public <b>electronic</b> communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as <b>home (fixed or wireless) networks or</b> corporate networks; <del>access</del> <b>or networks</b> to which <b>the access</b> is limited to a <b>pre-defined group of end-users, e.g. to family members or, members of the</b> corporation. <b>Similarly, this Regulation does not apply to data processed by services or networks used for purely internal communications purposes between public institutions, courts, court administrations, financial, social and employment administrations.</b> As soon as electronic communications data is transferred from a closed group network to a public electronic communications network, this Regulation applies to such data,	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>service as a whole is provided to an undefined group of end-users<del>the corporation.</del></i></p> <p>AM 11</p>	<p>including when it is M2M/IoT and personal/home assistant data. The provisions of this Regulation regarding the protection of end-users' terminal equipment information also apply in the case of terminal equipment connected to a closed group network such as a home (fixed or wireless) network which in turn is connected to a public electronic communications network.</p>	
Recital 14				
25	<p>(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</p>	<p>(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 <del>an end-user</del> <b>a user</b> 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. <b>It should also include data necessary</b></p>	<p>(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</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>	<p><b><i>to identify users' terminal equipment and data emitted by terminal equipment when searching for access points or other equipment.</i></b> 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. <b><i>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</i></b></p>	<p>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.</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>Regulation which applies to the providers of electronic communications services.</i></p> <p>AM 12</p>		
Recital 14a				
25a		<p><i>(14a) Modern electronic communications services, including the Internet and the OTT services that run on top of it, function on the basis of a protocol stack. Each protocol defines content (also called payload), a header and sometimes a trailer. Any higher protocol in the stack would be encapsulated in the content part of a lower level protocol. For example, A TCP segment would be in the content part of an IP packet, whose header would include the source and destination IP addresses between which the IP packet should be routed. TCP segments could contain an SMTP message in their content part, i.e. an e-mail. At the SMTP protocol level, the header would notably contain the sender and receiver email addresses and the content part would contain the message itself. In practice, the header and the trailer of a protocol message correspond to metadata for</i></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>the given protocol. This means that the metadata on one protocol layer will be content for the lower layers encapsulating the information. Where this Regulation lays down different rules for the processing of content and metadata, this should be understood specifically for the considered electronic communications service and the protocol layer it is operating on. For an Internet service provider, for example, the subject, the sender, the recipient and the body of an email will be altogether considered as content of the IP packets routed by it. However regarding an e-mail provider, only the subject and the body of the email will considered as content, whereas the recipient and the sender will be considered as metadata. This separation of protocol layers is crucial for maintaining the neutrality of the electronic communications services (net neutrality), which is protected under Regulation (EU) 2015/2120.</i></p> <p>AM 13</p>		
Recital 15				
26	(15) Electronic communications data should be treated as	(15) Electronic communications <del>data</del> should be treated as	(15) Electronic communications data should be treated as	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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</p>	<p>confidential. This means that any interference with the transmission of electronic communications <del>data</del>, 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. <b><i>When the processing is allowed under any exception to the prohibitions under this Regulation, any other processing on the basis of Article 6 of Regulation (EU) 2016/679 should be considered as prohibited, including processing for another purpose on the basis of Article 6 paragraph 4 of that Regulation. This should not prevent requesting additional consent for new processing operations.</i></b> The prohibition of interception of communications <del>data</del> should apply <b><i>also</i></b> during their conveyance. <b><i>For non-real-time electronic communications such as email or messaging, the transmission starts with the submission of the content for delivery and finishes with the, i.e. until</i></b> receipt of the content of the electronic communication by the <b><i>service provider of the intended addressee/recipient.</i></b> Interception of electronic communications <del>data</del> may occur, for example, when someone</p>	<p>confidential. This means that any interference <del>with the transmission of</del> electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of <del>all</del> the communicating parties should be prohibited. <del>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.</del> 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</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	(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.	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 <del>end-user</del> <b>user</b> 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 <del>end-user</del> <b>user</b> profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, <b>and analysis of users' traffic data</b> , including browsing habits without the <del>end-users</del> <b>users'</b> consent.  AM 14	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.	
Recital 15a				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
26a			<p><b>(15a) In order to ensure the confidentiality of electronic communications data, providers of electronic communications services should apply security measures in accordance with Article 40 of Directive (EU) 2018/1972 and Article 32 of Regulation (EU) 2016/679.</b></p> <p>Former 15aa</p>	
Recital 15b				
26b			<p><b>(15b) Moreover, trade secrets are protected in accordance with Directive (EU) 2016/943.</b></p> <p>Mandate 15aaa</p>	
Recital 15c				
26c			<p><b>(15c) The prohibition of interception of electronic communications content under this Regulation should apply until receipt of the content of the electronic communication by the intended addressee, i.e. during the end-to-end exchange of electronic communications content between end-users. Receipt implies that the end-user gains control over, and</b></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>has the possibility to interact with, the individual electronic communications content, for example by recording, storing, printing or otherwise processing such data, including for security purposes. The exact moment of the receipt of electronic communications content may depend on the type of electronic communications service that is provided. For instance, depending on the technology used, a voice call may be completed as soon as either of the end-users ends the call. For electronic mail or instant messaging, depending on the technology used, the moment of receipt may be as soon as the addressee has collected the message, typically from the server of the electronic communications service provider. Upon receipt, electronic communications content and related metadata should be erased or made anonymous in such a manner that no natural or legal person is identifiable, by the provider of the electronic communications service except when processing is permitted under this Regulation After electronic communications content has been received by the intended end-user or end-users, it may be</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			recorded or stored by those end-users. End-users are free to mandate a third party to record or store such data on their behalf.  Mandate 15a	
Recital 16				
27	(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. <b><i>It should not prohibit the processing of <del>in the</del> electronic communications network. It should not prohibit either the processing data by public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), providers of electronic communications data to ensure the networks and services and by providers of security technologies and services, in compliance with Regulation 2016/679 and to the extent strictly necessary and proportionate for the sole purposes of ensuring network and information security, i.e. preservation of availability,</i></b>	(16) The prohibition of <b>processing, including</b> storage of communications is not intended to prohibit any automatic, intermediate and transient <b>processing, including</b> storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications network. <b>Processing of electronic communications data by providers of electronic communications services and networks should only be permitted in accordance with this Regulation.</b> It should not prohibit <del>either</del> the processing of electronic communications data <b>without consent of the end-user</b> to ensure the security, <b>including the availability, authenticity, integrity or confidentiality, and continuity</b> of the electronic communications services, <del>for example including</del> checking security threats such as the presence of malware or <b>viruses, or</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>integrity], and confidentiality of information, and ensuring the security and continuity of the related services offered by, or accessible via, those networks and systems. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communications systems, security services, including checking security threats such as the presence of malware, spam or to check against DDoS attacks, or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc. Such processing could be carried out by another party which acts as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service.</i></p> <p>AM 15</p>	<p>the identification of phishing. Security measures are essential to prevent personal data breaches in electronic communications. Spam electronic messages may also affect the availability of the respective services and could potentially impact the performance of networks and services, which justifies the processing of electronic communications data to mitigate this risk. Such security measures, including anti-spam measures, should be proportionate and should be performed in the least intrusive manner. Providers of electronic communications services are encouraged to offer end-users the possibility to check electronic messages deemed as spam in order to ascertain whether they were indeed spam.</p> <p>the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc.</p>	
Recital 16a				
27a			(16a) The protection of the content of electronic communications pertains to the essence of the fundamental right	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>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 content 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 content, the provider of the electronic communications service should consult the supervisory authority if necessary pursuant to Article 36 (1) of Regulation (EU) 2016/679. Such consultation should be in accordance with</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content 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.	
Recital 16b				
27b			(16b) Services that facilitate end-users everyday life such as index functionality, personal assistant, translation services and services that enable more inclusion for persons with disabilities such as text-to-speech services are emerging. Processing of electronic communication content might be necessary also for some functionalities used normally in services for individual use, such as searching and organising the messages in email or messaging applications. Therefore, as regards the processing of electronic communications content for services requested by the end-user for their own individual use, consent should only be requested required from the end-user	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			requesting the service taking into account that the processing should not adversely affect fundamental rights and interest of another end-user concerned. Processing of electronic communications data should be allowed with the prior consent of the end-user concerned and to the extent necessary for the provision of the requested functionalities.	
Recital 16c				
27c			(16c) Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal person having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service in accordance with Regulation 2016/679.	
Recital 17				
28	(17) The processing of electronic communications data can be useful	(17) The processing of electronic communications data can be useful	(17) The processing of electronic communications <del>data</del> <b>metadata</b> can	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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</p>	<p>for businesses, consumers and society as a whole. <del>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.</del> However, <del>end-users</del><b>users</b> 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. <del>Therefore,</del> This Regulation should require providers of electronic communications services to obtain <del>end-users</del><b>users'</b> 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. <del>Examples of commercial usages of electronic communications metadata by providers of electronic communications services may</del></p>	<p>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, <del>based on end-users consent.</del> However, end-users attach great importance to the confidentiality of their communications, including their online activities, and <del>that they</del><b>they also</b> want to control the use of electronic communications <del>data</del><b>metadata</b> for purposes other than conveying the communication. Therefore, <del>this Regulation should require providers of electronic communications services to obtain end-users' consent</del><b>networks and services should be permitted 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 after having obtained the end-users' consent. In addition, those providers should be permitted to</b></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	<del>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.</del> 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.  AM 16	<b>process an end-user's electronic communications metadata where it is necessary for the provision of an electronic communications service based on a contract with that end-user and for billing related to that contract.</b> Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of <b>heatmaps</b> <del>heat maps</del> ; a graphical representation of data using <b>colors</b> <del>colours</del> 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,	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			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.	
Recital 17a				
28a		<i>(17a) 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</i>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure.</i></p> <p>AM 17</p>		
Recital 17a				
28b			<p><b>(17a) Further processing for purposes other than for which the metadata were initially collected may take place without the consent of the end-users concerned, provided that such processing is compatible with the purpose for which the metadata are initially collected, certain additional conditions and safeguards set out by this Regulation are complied with, including the requirement to genuinely anonymise the result before sharing the analysis with third parties. As end-users attach great value to the confidentiality of their communications, including their physical movements, such data cannot be used to determine the nature or characteristics on an end-user or to build a profile of an end-user, in order to, for example, avoid that the data is used for segmentation purposes, to monitor</b></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>the behaviour of a specific end-user or to draw conclusions concerning the private life of an end-user. For the same reason, the end-user must be provided with information about these processing activities taking place and given the right to object to such processing.</p> <p>Mandate 17aa</p>	
Recital 17b				
28c			<p>(17b) The processing of electronic communications metadata should also be regarded to be permitted where it is necessary in order to protect an interest which is essential for the life of the end-users who are natural persons or that of another natural person. Processing of electronic communications metadata for the protection of vital interests of the end-user may include for instance processing necessary for humanitarian purposes, including for monitoring epidemics and their spread or in humanitarian emergencies, in particular natural and man-made disasters. Processing of electronic communications metadata of an</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>end-user for the protection of the vital interest of an end-user who is a natural person should in principle take place only where the processing cannot be manifestly based on another legal basis and where the protection of such interests cannot be ensured without that processing.</p> <p>Mandate 17a</p>	
Recital 17c				
28d			<p>(17c) Processing of electronic communication metadata for scientific research or statistical purposes could also be considered to be permitted processing. This type of processing should be subject to safeguards to ensure privacy of the end-users by employing appropriate security measures such as encryption and pseudonymisation. In addition, end-users who are natural persons should be given the right to object. Processing for statistical and scientific purposes should only result in aggregated data, and not be used in support of measures or decisions regarding any particular natural person. In particular, such data should not be used to</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>determine the nature or characteristics of an end-user, to build an individual profile or to draw conclusions concerning an end-user private life. 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. Such usage should also include processing that is necessary for the development, production and dissemination of official national or European statistics in accordance with national or Union law, to the extent necessary for this purpose.</p> <p>Mandate 17b</p>	
Recital 18				
29	(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	(18) <del>End-users</del> <i>The user or end-user</i> 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-	(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	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>	<p>performance other than money, for instance by end-users being exposed to advertisements. For the purposes of this Regulation, consent of <del>an end-user, regardless of whether the latter is a natural or a legal person</del> <b>user</b>, 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. <b><i>Consent should not be considered as freely given if it is required to access any service or obtained through repetitive requests. In order to prevent such abusive requests, users should be able to order service providers to remember their choice not to consent and to adhere to technical specifications signalling not to consent, withdrawal of consent, or an objection.</i></b></p>	<p>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 <b>electronic communications</b> data from internet or voice communication usage will not be valid if the data subject <b>end-user</b> has no genuine and free choice, or is unable to refuse or withdraw consent without detriment.</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 18		
Recital 19				
30	<p>(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</p>	<p>(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 <del>interference with the processing of</del> content <b>data</b> 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 <del>end-users</del> <b>users</b> 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</p>	<p>(19) <del>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</del> <b>Third parties are legal or natural person that do not provide an</b> electronic communications <del>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 service to the end-user concerned. However,</del> <b>sometimes the same legal or natural person can also provide different kind of</b> services to <del>process electronic communications data in transit, with the informed consent of all the end-users concerned. the</del> <b>same end-user</b>, for example; <del>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</del></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>	<p>communications service should always <del>consult the supervisory authority prior to the processing.</del> <i>Such consultation should be in accordance with Article 36 (2) and (3) of carry out an impact assessment as provided for in Regulation (EU) 2016/679.</i> <del>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 and if</del> <b>necessary under that Regulation, consult the supervisory authority prior to the processing.</b> After electronic communications content has been sent by the <del>end-user</del><b>user</b> and received by the intended <del>end-user or end-users</del><b>user or users</b>, it may be recorded or stored by the <del>end-user, end-users</del><b>user, users</b> or by a third party entrusted by them to record or store such data, <b>which could be the electronic communications service provider.</b> Any processing of such <del>stored communications data where the data is stored on behalf of the user must comply with this Regulation.</del> <b>The user may further process the data and if it contains personal</b></p>	<p><del>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 information society service such as cloud storage. With respect to the provision of this other service, the same legal person is normally deemed to be a third party. If the other service is necessary for the provision of the electronic communications</del><b>communication</b> <del>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, such as automatic storage of the messages in the cloud by web-based email, the provider of such a service.</del> 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,</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><del>data, data</del> must comply with Regulation (EU) 2016/679.</p> <p>AM 19</p>	<p><del>end-users or by</del> normally is not deemed to be a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.</p>	
Recital 19a				
30a		<p><i>(19a) It should be possible to process electronic communications data for the purposes of providing services explicitly requested by a user for personal or personal work-related purposes such as search or keyword indexing functionality, virtual assistants, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools by persons with disabilities. This should be possible without the consent of all users but may take place with the consent of the user requesting the service. Such consent also precludes the provider from processing those data for other purposes.</i></p> <p>AM 20</p>		
Recital 19b				
30b				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>(19b) Interference with the confidentiality of metadata or interference with the protection of information stored in and related to end-users' terminal equipment can only be regarded to be lawful where it is strictly necessary and proportionate to protect an interest which is essential for the life of the data subject or that of another natural person. Such interference based on the vital interest of another natural person should take place only in a specific case and where the processing cannot be manifestly based on another legal basis.</i></p> <p>AM 21</p>		
Recital 20				
31	<p>(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</p>	<p>(20) Terminal equipment of <del>end-users</del><b>users</b> 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 <del>end-users</del><b>users</b> requiring protection under the</p>	<p>(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, <del>whether in particular</del> <b>where such information is processed by, is stored in, or collected from or emitted by</b> such equipment, <del>requested from or</del> <b>where information is collected from it</b> or processed in order to enable it to connect to another device and or</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>	<p>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 <del>information</del> <b>very sensitive data</b> that may reveal details of <del>an individual's emotional, political, social complexities</del> <b>behaviour, psychological features, emotional condition and preferences of an individual</b>, including the content of communications, pictures, the location of individuals by accessing the <del>device's</del> <b>of the device</b> GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. <del>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.</del> Information related to the <del>end-user</del> <b>user's</b> device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often</p>	<p>network equipment, are part of the <b>end-user's</b> private sphere, <b>including the privacy of one's communications, and require of the end-users</b> requiring protection <del>under</del> <b>in accordance with</b> the Charter of Fundamental Rights of the European Union <del>and the European Convention for the Protection of Human Rights and Fundamental Freedoms.</del> 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</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>	<p>without the knowledge of the end-user, and may seriously intrude upon the privacy of these <del>end-users</del>users. <i>Furthermore, so-called spyware, web bugs, hidden identifiers and unwanted tracking tools can enter users' terminal equipment without their knowledge in order to gain access to information or to store hidden information, to process data and use input and output functionalities such as sensors, and to trace the activities.</i> Techniques that surreptitiously monitor the actions of <del>end-users</del>users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the <del>end-users</del>users' terminal equipment pose a serious threat to the privacy of <del>end-users</del>users. Therefore, any such interference with the <del>end-user</del>user's terminal equipment should be allowed only with the <del>end-user</del>user's consent and for specific and transparent purposes. <i>Users should receive all relevant information about the intended processing in clear and easily understandable language. Such information should be provided separately from the terms and conditions of the service.</i></p> <p>AM 22</p>	<p>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, <del>any such interference with the</del> <b>the use of processing and storage capabilities and the collection of information from</b> end-user's terminal equipment should be allowed only with the end-user's consent <b>or for other</b> <del>and for</del> specific and transparent purposes <b>as laid down in this Regulation. The information collected from end-user's terminal equipment can often contain personal data.</b></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Recital 20a				
31a			<p>(20a) In light of the principle of purpose limitation laid down in Article 5 (1) (b) of Regulation (EU) 2016/679, it should be possible to process in accordance with this Regulation data collected from the end-user's terminal equipment for purposes compatible with the purpose for which it was collected from the end-user's terminal equipment.</p> <p>Mandate 20aa</p>	
Recital 20b				
31b			<p>(20b) The responsibility for obtaining consent for the storage of a cookie or similar identifier lies on the entity that makes use of processing and storage capabilities of terminal equipment or collects information from end-users' terminal equipment, such as an information society service provider or ad network provider. Such entities may request another party to obtain consent on their behalf. The end-user's consent to storage of a cookie or similar identifier may also entail consent</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			for the subsequent readings of the cookie in the context of a revisit to the same website domain initially visited by the end-user.  Mandate 20aaa	
Recital 20c				
31c			(20c) In contrast to access to website content provided against monetary payment, where access is provided without direct monetary payment and is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases,	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. This would normally be the case for websites providing certain services, such as those provided by public authorities. Similarly, such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position.</p> <p>To the extent that use is made of processing and storage capabilities of terminal equipment and information from end-users' terminal equipment is collected for other purposes than for what is necessary for the purpose of providing an electronic communication service or for the provision of the service requested, consent should be required. In such a scenario, consent should normally be given by the end-user who requests the service from the provider of the service.</p> <p>Mandate 20aaaa</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Recital 20d				
31d			<p>(20d) End-users are often requested to provide consent to the storage and access to stored data in their terminal equipment, due to the ubiquitous use of tracking cookies and similar tracking technologies. As a result, end-users may be overloaded with requests to provide consent. This can lead to a situation where consent request information is no longer read and the protection offered by consent is undermined. Implementation of technical means in electronic communications software to provide specific and informed consent through transparent and user-friendly settings, can be useful to address this issue. Where available and technically feasible, an end user may therefore grant, through software settings, consent to a specific provider for the use of processing and storage capabilities of terminal equipment for one or multiple specific purposes across one or more specific services of that provider. For example, an end-user can give consent to the use of certain types of cookies by</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>whitelisting one or several providers for their specified purposes. Providers of software are encouraged to include settings in their software which allows end-users, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment. In light of end-user's self-determination, consent directly expressed by an end-user should always prevail over software settings. Any consent requested and given by an end-user to a service should be directly implemented, without any further delay, by the applications of the end user's terminal. If the storage of information or the access of information already stored in the end-user's terminal equipment is permitted, the same should apply.</p> <p>Mandate 20a</p>	
Recital 21				
32	(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities	(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities	(21) <del>Exceptions to the obligation to obtain consent to make</del> Use of the processing and storage capabilities	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>	<p>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 <del>authorizing</del><b>authorising</b> 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 <del>end-user</del><b>user</b>. This may include the storing of <b>information (such as cookies and other identifiers)</b> 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. <del>Cookies</del><b>Such techniques, if implemented with appropriate privacy safeguards,</b> can also be a legitimate and useful tool, for example, in measuring web traffic to a website. <b>Such measuring implies that the result of processing is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.</b> Information society providers <del>that could</del> engage in configuration checking <b>in order</b> to provide the</p>	<p>of terminal equipment or <del>to access</del> <b>to</b> information stored in terminal equipment <b>without the consent of the end-user</b> 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 <del>strictly</del> necessary and proportionate for the <del>legitimate</del> purpose of <del>enabling the use of</del><b>providing</b> a specific service <del>explicitly</del> 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., <b>authentication session</b> cookies <del>can</del> 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 <b>used to verify the identity of end-users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket. In the area of IoT services</b></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p>service in compliance with the <del>end-user</del> user's settings and the mere logging <del>of revealing</del> the fact that the <del>end-user</del> user's device is unable to receive content requested by the <del>end-user</del> user, should not constitute <b>illegitimate</b> access to such a device, or use of the device processing capabilities <b>for which consent is required</b>.</p> <p>AM 23</p>	<p><b>which rely on connected devices (such as connected thermostats, connected medical devices, smart meters or automated and connected vehicles), the use of the processing and storage capacities of those devices and access to information stored therein should not require consent to the extent that such use or access is necessary for the provision of the service requested by the end-user. For example, storing of information in or accessing information from a smart meter might be considered as necessary for the provision of a requested energy supply service to the extent the information stored and accessed is necessary for the stability and security of the energy network or for the billing should not constitute access to such a device or use of the device end-users' energy consumption. The same applies for instance to storing, processing capabilities or accessing of information from automated and connected vehicles for security related software updates.</b></p>	
Recital 21a				
32a			<b>(21a) In some cases the use of processing and storage capabilities</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing a service, requested by the end-user, such as services provided in accordance with the freedom of expression and information including for journalistic purposes, e.g. online newspaper or other press publications as defined in Article 2 (4) of Directive (EU) 2019/790, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar techniques and has accepted such use.</p> <p>Mandate 21aa</p>	
Recital 21b				
32b			<p>(21b) Cookies can also be a legitimate and useful tool, for example, in assessing the effectiveness of a delivered information society service, for example of website design and advertising or by helping to measure the numbers of end-users</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>visiting a website, certain pages of a website or the number of end-users of an application. This is not the case, however, regarding cookies and similar identifiers used to determine the nature of who is using the site, which always require the consent of the end-user. 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.</p> <p>Mandate 21a</p>	
Recital 21c				
32c			<p>(21c) Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs or for software-updates for security reasons, provided that the end-user concerned has been informed prior to such updates, and</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p>provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception.</p> <p>Mandate 21b</p>	
Recital 22				
33	<p>(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-</p>	<p>(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, <del>end-users</del><b>users</b> are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, <del>end-users</del><b>users</b> are overloaded with requests to provide consent. <b><i>This Regulation should prevent the use of so- called "cookie walls" and</i></b></p>	<p>Deleted</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	<i>"cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.</i> 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 <i>technical specifications, for instance by</i> using the appropriate settings of a browser or other application. <i>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.</i> The choices made by <del>end-users</del> users when establishing <del>its</del> the general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><del>end-user</del>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, <i>or applications or operating systems</i> may be used as <del>gatekeepers</del><i>the executor of a user's choices</i>, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.</p> <p>AM 24</p>		
Recital 23				
34	<p>(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</p>	<p>(23) The principles of data protection by design and by default <del>were</del><i>are</i> 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 <del>enabling the retrieval and presentation of information on the internet should have an obligation to</del><i>permitting electronic communications (such as browsers, operating systems and</i></p>	Deleted	<p>(25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>	<p><i>communication apps), irrespective of whether the software is obtained separately or bundled with hardware, shall configure the software so that <del>it offers the option to prevent third parties from storing</del> privacy is protected, the cross- domain tracking and the storing of information on the terminal equipment; <del>this is often presented as ‘reject third party cookies’</del>. End-users should be offered a set of privacy setting options, ranging from higher (for example, ‘never accept cookies’ by third parties is prohibited by default. In addition, providers of such software are required to offer sufficiently granular options to consent to each distinct category of purposes. These distinct categories include, at least, the following categories: (i) tracking for commercial purposes or for direct marketing for non-commercial purposes (behavioural advertising); (ii) tracking for personalised content; (iii) tracking for analytical purposes; (iv) tracking of location data; (v) providing personal data to third parties (including providing unique identifiers to match with personal data held by third parties) No consent is required for information that is collected from</i></p>		<p>and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>end-users' terminal equipment when it is strictly necessary for providing an information society service requested by the end-user, <del>to</del> <del>lower</del> (for example in order to adapt the screen size to the device, or to remember items in a shopping basket. Web browsers, operating systems and communication apps should allow the end-user to consent to, 'always accept cookies' or other information that is stored on, or read from terminal equipment (including the browser on that equipment) by a specific website or originator even when the general settings prevent the interference and vice versa. With regard to a specific party, web browsers and communication apps should also allow users to separately consent to internet-wide tracking. Privacy settings should also include options to allow the user to decide and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies') whether multimedia players, interactive programming language viewers, or similar software can be executed, if a website can collect geo-location data from the user, or if it can access specific hardware such as a webcam or microphone. Such</i></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p>privacy settings should be presented in <del>an</del> an easily visible and intelligible manner, <i>and at the moment of installation or first use, users should be informed about the possibility to change the default privacy settings among the various options. Information provided should not dissuade users from selecting higher privacy settings and should include relevant information about the risks associated to allowing cross-domain trackers, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising or sharing with more third parties. Software manufacturers should be required to provide easy ways for users to change the privacy settings at any time during use and to allow the user to make exceptions for or to specify for such services websites trackers and cookies are always or never allowed.</i></p> <p>AM 25</p>		
Recital 24				
35	(24) For web browsers to be able to obtain end-users' consent as defined	(24) <del>For web browsers to be able to obtain end-users' consent as defined</del>	Deleted	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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</p>	<p><del>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</del></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	<del>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.</del>  AM 26 deleted		
Recital 25				
36	(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	(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	(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, <b>the WiFi signal</b> 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	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>	<p>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 <del>end-users</del><b>users</b>, for example when they enter stores, with <del>personalized</del><b>personalised</b> 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 <del>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</del><b>either obtain the user's consent or anonymise the data immediately while limiting the purpose to mere statistical counting</b> within a <del>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</del></p>	<p>captured. Service providers have emerged who offer <b>physical movements'</b> tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, <b>such as</b> providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. <del>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</del><b>referred to as statistical counting for which the consent of end-users is not needed, provided that such counting is limited in time and space to the extent necessary for this purpose. Providers should also apply appropriate technical and organisations measures to ensure the level if security appropriate to the risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations</b><b>including pseudonymisation of the data and making it anonymous or erase it as soon it is not longer needed for this purpose.</b> Providers engaged in</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><del>stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679</del> <b>limited time and space and offering effective opt-out possibilities.</b></p> <p>AM 27</p>	<p>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. <b>This information may be used for more intrusive purposes, which should not be considered statistical counting, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers locations, subject to the conditions laid down in this Regulation, as well as the tracking of individuals over time, including repeated visits to specified locations.</b></p>	
Recital 25a				
36a			<b>(25a) Processing the information emitted by the terminal equipment to enable it to connect to another</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			device would be permitted if the end-user has given consent or if it is necessary for the provision of a service requested by the end-user. This kind of processing might be necessary for example for the provision of some IoT related services.	
Recital 26				
37	(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State,	(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security <del>and other important objectives of general public interest of the Union or of a Member State,</del>	(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, <b>including by way of derogations,</b> when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including <del>national security, defence,</del> 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	(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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).</p>	<p><del>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.</del> 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. <del>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).</del></p> <p>AM 28</p>	<p>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, <b>including by requiring providers to enable and assist competent authorities in carrying out lawful interceptions,</b> or take other measures, <b>such as legislative measures providing for the retention of data for a limited period of time,</b> 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</p>	<p>these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			role of the representative designated pursuant to Article 3(3).	
Recital 26a				
37a		<p><i>(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".</i></p> <p>AM 29</p>		
Recital 27				
38	(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		(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	(34) It is necessary, as regards calling line identification, 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

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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.</p>		<p>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.</p>	<p>from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, 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, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
				available electronic communications service.
Recital 28				
39	(28) There is justification for overriding the elimination of calling line identification presentation in specific cases. End-users' rights to privacy with regard to calling line identification should be restricted where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services, such as eCall, to carry out their tasks as effectively as possible.		(28) There is justification for overriding the elimination of calling line identification presentation in specific cases. End-users' rights to privacy with regard to calling line identification should be restricted where this is necessary to trace <b>malicious or</b> 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. <b>Location information established by the terminal equipment, using its built-in Global Navigation Satellite Systems (GNSS) capabilities or other types of terminal equipment based location data, such as location data derived from the WiFi functionality, may supplement the location data supplied by providers of number-based interpersonal communications services when a call is made to emergency services. The temporary denial or absence of consent of an end-user to access location data provided by the terminal equipment GNSS, for</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			example, because location settings are turned off, shall not prevent the transfer of such information to emergency services for the purposes of facilitating access to such services. Directive 2014/53/EU empowers the Commission to adopt delegated acts requiring that specific categories or classes of radio equipment support certain features ensuring access to emergency services.	
Recital 29				
40	(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, <b>malicious or nuisance</b> calls by end-users in different ways, including blocking silent calls and other <del>fraudulent</del> <b>unwanted, malicious</b> and nuisance calls, <b>such as calls originating from invalid numbers, i.e. numbers that do not exist in the numbering plan, valid numbers that are not allocated to a provider of a number-based interpersonal communications service, and valid numbers that are allocated but not assigned to an end-user. Providers of-</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			Providers of publicly available number-based interpersonal communications services should deploy this technology and protect end-users against <del>nuisance</del> <b>such</b> 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.	
Recital 30				
41	(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 <del>end-users that are natural persons</del> <b>users</b> 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. <b>The consent should</b>	(30) <del>Publicly available directories of end-users of electronic communications services are widely distributed.</del> Publicly available directories means any directory or service containing <b>information on end-users information of number-based interpersonal communication services</b> such as <b>name</b> , phone numbers (including mobile phone numbers), email address, <del>home address contact details</del> and includes inquiry services. <del>The right to privacy and to protection of the personal data of a natural person requires that,</del> <b>the main function of which is to enable to identify such end-users.</b> End-users that are natural persons <del>are</del> <b>should be</b> asked for consent before their personal data are	(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>be collected by the electronic communications service provider at the moment of signing the contract for such service. Natural persons acting in a professional capacity, such as independent professionals, operators of small businesses or freelancers, shall be equated with legal persons, as regards their data related to their professional capacity.</i></p> <p>AM 30</p>	<p>included in a directory, <b>unless Member States provide that such end-users have the right to object to inclusion of their personal data.</b></p> <p>The legitimate interest of legal <del>entities</del>persons requires that end-users that are legal <del>entities</del>persons have the right to object to the data related to them being included in a directory. <b>End-users who are natural persons acting in a professional capacity should be treated as legal persons for the purpose of the provisions on publicly available directories.</b></p>	<p>telephone number only.</p>
Recital 31				
42	<p>(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</p>	<p>(31) <del>If end-users that are natural persons</del> <b>If users</b> 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, <del>providers of publicly available directories</del><b>electronic communications service providers</b> should inform the <del>end-users</del><b>users</b> of the purposes of the directory and of the search functions of the directory before including them in that</p>	<p>(31) <del>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).</del> In addition, Providers of publicly available directories<b>number-based interpersonal communications services</b> should inform the end-users <del>of the purposes of the directory and</del><b>who are natural persons</b> of the search functions of the directory</p>	<p>(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	directory. <del>End-users</del> <b>Users</b> 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 <del>end-user</del> <b>user's</b> contact details can be searched should not necessarily be the same. <b><i>The providers or publicly available directories shall provide information about the search functions, as well as if new options and functions of the directories are available in the publicly available directories and provide the users the option to disable such functions.</i></b>  <a href="#">AM 31</a>	<del>before including them in that directory. End-users should be able to determine by consent on the basis of which categories of</del> <b>and obtain their consent before enabling such search functions related to their personal data—their contact details can be searched.</b> 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.	party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.
Recital 32				
43	(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	(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, <b><i>regardless of the form it takes.</i></b> In addition to the offering of products and services for commercial purposes, this should	(32) In this Regulation, direct marketing <b>communications</b> refers to any form of advertising <del>by which</del> <b>sent by</b> a natural or legal person <del>sends</del> <b>directly to one or more specific end-users using publicly available electronic communications services.</b> <b>The provisions on direct marketing communications should not apply to other form of</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	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.  AM 32	<b>marketing or advertising that is not sent</b> directly to <del>one or more identified or identifiable end-users</del> using electronic communications services <b>any specific end-user for reception by that end-user at addresses, number or other contact details, e.g. the display of advertising on a visited website or within an information society service requested by that end-user.</b> In addition to <b>direct communications advertising</b> for the offering of products and services for commercial purposes, <del>this should also</del> <b>Member States may decide that direct marketing communications may include messages</b> <b>direct marketing communications</b> sent by political parties that contact natural persons via <b>publicly available</b> electronic communications services in order to promote their parties. The same <del>should apply</del> <b>applies</b> to messages sent by other non-profit organisations to support the purposes of the organisation.	
Recital 33				
44	(33) Safeguards should be provided to protect end-users against unsolicited communications for	(33) Safeguards should be provided to protect end-users against unsolicited communications <del>for</del> <b>or</b>	(33) Safeguards should be provided to protect end-users against <del>unsolicited communications for</del>	(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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</p>	<p>direct marketing <del>purposes</del>, 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 <del>communication</del><b>communications systems, semi-automated</b> systems, instant messaging applications, <del>emails</del><b>faxes, e-mails</b>, 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 <b>and</b> 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 <b>high</b> level of protection for all <del>citizens</del><b>end-users</b> throughout the</p>	<p>direct marketing <del>purposes</del><b>communications</b>, which intrude into the <del>private life</del><b>privacy</b> 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 <del>end-user is obtained before commercial electronic communications for</del><b>end-users who are natural persons is obtained before</b> direct marketing <del>purposes</del><b>communications</b> are sent to <del>end-users</del><b>them</b> in order to effectively protect <del>individuals</del><b>them</b> against the intrusion into their private life <del>as well as the legitimate interest of legal persons</del>. Legal certainty and the need to ensure that the rules protecting against <del>unsolicited electronic</del><b>direct marketing</b> communications remain future-proof justify the need to define <b>in principle</b> a single set of rules that do not vary according to the technology used to convey these <del>unsolicited</del><b>direct marketing</b> communications, while at the same</p>	<p>purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.</p> <p>(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	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 <del>similar</del> <b>other</b> 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.  AM 33	time guaranteeing an equivalent level of protection for all citizens throughout the Union. However, it is reasonable to allow the use of <del>e-mail</del> contact details <b>for electronic message</b> 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 <del>electronic</del> contact details <b>for electronic message</b> in accordance with Regulation (EU) 2016/679.	informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.
Recital 34				
45	(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 and		(34) When end-users <b>who are natural persons</b> have provided their consent to receiving <del>unsolicited communications for direct marketing purposes</del> <b>communications</b> , they should still be able to withdraw their consent at any time in an easy manner <b>and without any cost to them</b> . To facilitate effective enforcement of Union rules on <del>unsolicited messages for direct marketing</del> <b>communications</b> , it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending <del>unsolicited commercial communications for</del>	(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.		direct marketing purposes. <del>Unsolicited communications.</del> <b>Direct</b> marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person <del>transmitting</del> <b>sending</b> the communication <del>or on</del> <b>and, where applicable, on whose behalf of whom</b> the communication is <del>transmitted</del> <b>sent</b> and provide the necessary information for <del>recipients</del> <b>end-users who are natural persons</b> to exercise their right to <del>oppose</del> <b>withdraw their consent</b> to receiving further <del>written and/or oral marketing messages</del> <b>direct marketing communications, such as valid contact details (e.g. link, e-mail address) which can be easily used by end-users who are natural persons to withdraw their consent free of charge.</b>	
Recital 35				
46	(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		(35) <del>In order to allow easy withdrawal of consent,</del> Legal or natural persons conducting direct marketing communications <b>through voice-to-voice calls and through calls by automating calling and communication systems should</b>	(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.		<del>present their identity line only email should present a link, or a valid electronic mail address, which the company 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 called.</del> <b>Member States are encouraged to introduce by means of national law a specific code or prefix identifying the fact that the call is a direct marketing call to improve the tools provided for the end-users in order to protect their privacy in more efficient manner.</b> Using a specific code identifying the fact that the call is a or prefix should not relieve the legal or natural persons sending direct marketing call from the obligation to present their calling line identification.	costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.
Recital 36				
47	(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	(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and <del>communication</del> communications systems, given that they are more	<del>(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</del>	(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.	costly for the sender and impose no financial costs on end-users- <del>Member States should therefore be able,</del> <b>justify the obligation for Member States</b> to establish and or maintain national systems only allowing such calls to end-users who have not objected.  AM 34	<del>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.</del> <b>certain types of voice-to-voice calls to end-users who are natural persons and who have not objected, including in the context of an existing customer relationship.</b>  Mandate 33a	calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.
Recital 37				
48	(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	(37) Service providers who offer electronic communications services should <del>inform end-process</del> <b>electronic communications data in such a way as to prevent unauthorised processing, including access, or alteration. They should ensure that such unauthorised access or alteration can be detected, and also ensure that electronic communications data are protected by using state-of the art software and cryptographic methods including encryption technologies. Service providers should also inform</b> users of measures they can take to protect the security of their communications for instance by using specific types of software or	Deleted	(20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	light of Article 32 of Regulation (EU) 2016/679.	<p>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. <i><b>The obligations of Article 40 of the [European Electronic Communications Code] should apply to all services within the scope of this Regulation as regards the security of networks and services and related security obligations thereto.</b></i></p> <p>AM 35</p>		<p>available electronic communications services over the Internet should inform users and subscribers 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 subscribers 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 except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.</p>
Recital 38				
49	(38) To ensure full consistency with Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions	(38) To ensure full consistency with Regulation (EU) 2016/679, The enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions	(38) <del>To ensure full consistency with Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation should be entrusted to the same</del> <b>Member States should be able to have more than one</b>	

	Commission Proposal	EP Mandate	<div>st6087/21</div> <div>Council Mandate</div>	Directive 2002/58/EC
	<p>Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.</p>	<p>Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. <i>Where more than one supervisory authority is established in a Member State, such authorities should cooperate with each other. They should also cooperate with the authorities appointed to enforce the European Electronic Communications Code and other relevant enforcement authorities, such as the authorities tasked with consumer protection.</i> Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this</p>	<p><b>supervisory authority, to reflect their constitutional, organisational and administrative structure. The designation of supervisory authorities responsible for the enforcement monitoring of the provisions Regulation (EU) 2016/679 and application of this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able cannot affect the right of natural persons to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for compliance with rules regarding the protection of personal data subject to control by an independent authority in accordance with Article 8(3) of the Charter as interpreted by the Court. End-users who are legal entities. Such additional tasks persons should not jeopardise the ability of the supervisory authority to perform its tasks have the same rights as end-users who are natural persons regarding the protection of personal data under Regulation (EU) 2016/679 and any</b></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		Regulation. <a href="#">AM 36</a>	<b>supervisory authority entrusted to monitor any provisions of</b> this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the <b>additional tasks designated</b> under this Regulation.	
Recital 38a				
49a		<i>(38a) The enforcement of the provisions of this Regulation often requires cooperation between the national supervisory authorities of two or more Member States, for example in combating interferences with the confidentiality of the terminal equipment. In order to ensure a smooth and rapid cooperation in such cases, the procedures of the cooperation and consistency mechanism established under Regulation 2016/679/EU should apply to Chapter II of this Regulation. Therefore, the European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, in particular by issuing opinions in the context of the consistency mechanisms or by</i>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>adopting binding decisions in the context of dispute resolution as provided in Article 65 of Regulation 2016/679/EU, as regards Chapter II of this Regulation.</i></p> <p>AM 37</p>		
Recital 39				
50	<p>(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.</p>	<p>(39) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks, <b><i>including adopting binding decisions</i></b>, 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, <b><i>including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers</i></b>, 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</p>	<p>(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. <del>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.</del> 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.</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.  AM 38		
Recital 40				
51	(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		(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	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	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.		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.	
Recital 41				
52	(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	(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons <b><i>in the provision and use of electronic communications services</i></b> and in particular their right to <del>the</del> <b><i>protection-respect of their private life and communications with regard to the processing</i></b> 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,	(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. <del>Delegated acts are also necessary to specify a</del>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	<p>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<sup>1</sup>. 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.</p> <p><sup>1</sup>. 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).</p>	<p>the person responsible for it and of any measure the <del>end-user</del> <b>user</b> of the terminal equipment can take to minimise the collection. <del>Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems.</del> 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<sup>1</sup>. 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. <b>For instance, implementing measures are necessary to specify a code to</b></p>	<p><del>code to identify direct marketing calls including those made through automated calling and communication systems.</del> 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<sup>11</sup>. 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.</p> <p><del><sup>1</sup>. 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).</del></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>identify direct marketing calls including those made through automated calling and communications systems. They are also necessary to establish the procedures and circumstances to override the elimination of the presentation of the calling line identification on a temporary basis where users request the tracing of malicious or nuisance calls.</i> Those powers should be exercised in accordance with Regulation (EU) No 182/2011.</p> <p>1. 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).</p> <p>AM 39</p>		
Recital 42				
53	(42) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural and legal persons and the free flow of electronic communications data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better		(42) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural and legal persons and the free flow of electronic communications data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.		achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	
Recital 43				
54	(43) Directive 2002/58/EC should be repealed.		(43) Directive 2002/58/EC should be repealed.	
Formula				
55	HAVE ADOPTED THIS REGULATION:		HAVE ADOPTED THIS REGULATION:	
CHAPTER I				
56	CHAPTER I GENERAL PROVISIONS		CHAPTER I GENERAL PROVISIONS	
Article 1				
57	Article 1 Subject matter		Article 1 Subject matter	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 1(1)				
58	1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.		1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of <del>natural and legal</del> persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.	1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.
Article 1(1a)				
58a			<b>1a. This Regulation lays down rules regarding the protection of the fundamental rights and freedoms of legal persons in the provision and use of the electronic communications services, and in particular their rights to respect of communications.</b>	
Article 1(2)				
59	2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, which shall be neither restricted nor prohibited for reasons		2. <del>This Regulation ensures</del> <b>The</b> free movement of electronic communications data and electronic communications services within the Union, <del>which</del> shall be neither restricted nor prohibited for reasons	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data.		related to the respect for the private life and communications of natural <del>and legal</del> persons and the protection of natural persons with regard to the processing of personal data, <b>and for protection of communications of legal persons.</b>	
Article 1(3)				
60	3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.		3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 <del>and to</del> 2.	2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.
Article 2				
61	Article 2 Material Scope		Article 2 Material Scope	
Article 2(1)				
62	1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.	1. This Regulation applies to <del>the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.:</del>	1. This Regulation applies to <del>the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.:</del>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 40		
Article 2(1), point (a)				
62a		<p><i>(a) the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services, irrespective of whether a payment is required;</i></p> <p>AM 41</p>	<p><b>(a) the processing of electronic communications content and of electronic communications metadata carried out in connection with the provision and the use of electronic communications services;</b></p>	
Article 2(1), point (b)				
62b		<p><i>(b) the processing of information related to or processed by the terminal equipment of end-users;</i></p> <p>AM 42</p>	<p><b>(b) end-users' terminal equipment information</b></p>	
Article 2(1), point (c)				
62c		<p><i>(c) the placing on the market of software permitting electronic communications including the retrieval and presentation of information on the Internet;</i></p> <p>AM 43</p>		
Article 2(1), point (d)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
62d		<p><i>(d) the provision of publicly available directories of users of electronic communications;</i></p> <p>AM 44</p>	<p><b>(c) the offering of a publicly available directory of end-users of electronic communications services;</b></p> <p>Mandate Art 2(1)(c)</p>	
Article 2(1), point (e)				
62e		<p><i>(e) the sending of direct marketing electronic communications to end-users.</i></p> <p>AM 45</p>	<p><b>(d) the sending of direct marketing communications to end-users</b></p> <p>Mandate Art 2(1)(d)</p>	
Article 2(2), introductory part				
63	2. This Regulation does not apply to:		2. This Regulation does not apply to:	
Article 2(2), point (a)				
64	(a) activities which fall outside the scope of Union law;		<p>(a) activities, which fall outside the scope of Union law, <b>and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority;</b></p>	3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
				activities relate to State security matters) and the activities of the State in areas of criminal law.
Article 2(2), point (b)				
65	(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;		(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;	
Article 2(2), point (c)				
66	(c) electronic communications services which are not publicly available;		(c) electronic communications services which are not publicly available;	
Article 2(2), point (d)				
67	(d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;		(d) activities, <b>including data processing activities</b> , of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;	
Article 2(2), point (e)				
67a			<b>(e) electronic communications</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			data processed after receipt by the end-user concerned.	
Article 2(2), point (e)				
68	(e) THIS POINT IS MISSING. THANK YOU FOR USING ANOTHER LANGUAGE.	The point (e) does not exist in English language. It is a byproduct of XMLisation from MS Word, and should be disregarded.	deleted	
Article 2(3)				
69	3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001].		3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001] 2018/1725 .	
Article 2(4)				
70	4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC <sup>1</sup> , in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.  <sup>1</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information		4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC <sup>1</sup> , in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.  <sup>1</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1–16).		society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1–16).	
Article 2(5)				
71	5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.		5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.	
Article 3				
72	Article 3 Territorial scope and representative	Article 3 Territorial scope and representative	Article 3 Territorial scope and representative	
Article 3(1), introductory part				
73	1. This Regulation applies to:		1. This Regulation applies to:	
Article 3(1), point (a)				
74	(a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;	(a) the <del>provision</del> <b>offering</b> of electronic communications services, <b>software, publicly available directories, or direct marketing electronic communications</b> to end-users in the Union, irrespective of whether a payment of the end-user is required;  AM 46	(a) the provision of electronic communications services to end-users <b>who are</b> in the Union, <del>irrespective of whether a payment of the end-user is required;</del>	1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 3(1), point (aa)				
74a			(aa) the processing of electronic communications content and of electronic communications metadata of end-users who are in the Union;	
Article 3(1), point (b)				
75	(b) the use of such services;	(b) the <del>use of such services</del> <i>activities referred to in Article 2 that are provided from the territory of the Union;</i>  AM 47	Deleted	
Article 3(1), point (c)				
76	(c) the protection of information related to the terminal equipment of end-users located in the Union.	(c) the <del>protection</del> <i>processing</i> of information related to <i>or processed by</i> the terminal equipment of end-users <del>located</del> <i>that is</i> in the Union.  AM 48	(c) the protection of <del>information</del> <i>information</i> related to the terminal equipment <del>located</del> <i>who are</i> in the Union.	
Article 3(1), point (cb)				
76a			(cb) the offering of publicly available directories of end-users of electronic communications	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			services who are in the Union;	
Article 3(1), point (cc)				
76b			(cc) the sending of direct marketing communications to end-users who are in the Union.	
Article 3(2)				
77	2. Where the provider of an electronic communications service is not established in the Union it shall designate in writing a representative in the Union.	2. Where the provider of an electronic communications service, <i>provider of software permitting electronic communications, a person processing information related to or processed by the terminal equipment of users or end-users, a provider of a publicly available directory, or a person using electronic communications services to transmit direct marketing communications</i> is not established in the Union, it shall designate in writing a representative in the Union. <a href="#">AM 49</a>	2. Where the provider of an electronic communications service, <b>the provider of a publicly available directory, or a person using electronic communications services to send direct marketing communications, or a person using processing and storage capabilities or collecting information processed by or emitted by or stored in the end-users' terminal equipment</b> is not established in the Union it shall designate in writing, <b>within one month from the start of its activities</b> , a representative in the Union <b>and communicate it to the competent Supervisory Authority.</b>	
Article 3(2a)				
77a			<b>2a. The requirements laid down in paragraph 2 shall not apply if</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			activities listed in paragraph 1 are occasional and are unlikely to result in a risk to the fundamental rights of end-users taking into account the nature, context, scope and purpose of those activities.	
Article 3(3)				
78	3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.		3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.	
Article 3(4)				
79	4. The representative shall have the power to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.	4. The representative shall have the power to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, <b><i>courts</i></b> , and end-users, on all issues related to <del>processing electronic communications data</del> <b><i>the activities referred to in Article 2</i></b> for the purposes of ensuring compliance with this Regulation.  AM 50	4. The representative shall <del>have the power to answer questions and provide information</del> <b>be mandated by the provider or person it represents to be addressed</b> in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.	
Article 3(5)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
80	5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against a natural or legal person who processes electronic communications data in connection with the provision of electronic communications services from outside the Union to end-users in the Union.	5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against a natural or legal person who <del>processes electronic communications data in connection with the provision of electronic communications services</del> <b>undertakes the activities referred to in Article 2</b> from outside <del>the Union to end-users</del> <b>in</b> the Union.  AM 51	5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against <del>a natural or legal</del> <b>the provider or</b> person who processes electronic communications data in connection with the provision of electronic communications services from outside the Union to end-users <b>in the Union it represents.</b>	
Article 3(5a)				
80a			<b>5a. This Regulation applies to the processing of personal data by a provider not established in the Union, but in a place where Member State law applies by virtue of public international law.</b>  Mandate Art 3(6)	
Article 4				
81	Article 4 Definitions	Article 4 Definitions	Article 4 Definitions	
Article 4(1), introductory part				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
82	1. For the purposes of this Regulation, following definitions shall apply:		1. For the purposes of this Regulation, following definitions shall apply:	Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)(8) shall apply.
Article 4(1), point (a)				
83	(a) the definitions in Regulation (EU) 2016/679;		(a) the definitions in Regulation (EU) 2016/679;	
Article 4(1), point (b)				
84	(b) the definitions of ‘electronic communications network’, ‘electronic communications service’, ‘interpersonal communications service’, ‘number-based interpersonal communications service’, ‘number-independent interpersonal communications service’, ‘end-user’ and ‘call’ in points (1), (4), (5), (6), (7), (14) and (21) respectively of Article 2 of [Directive establishing the European Electronic Communications Code];	(b) the <del>definitions</del> <b>definition</b> of ‘ <del>electronic communications network</del> ’, ‘ <del>electronic communications service</del> ’, ‘ <del>interpersonal communications service</del> ’, ‘ <del>number-based interpersonal communications service</del> ’, ‘ <del>number-independent interpersonal communications service</del> ’, ‘ <del>end-user</del> ’ and ‘ <del>call</del> ’ in <del>points (1), (4), (5), (6), (7), (14) and (21) respectively</del> <b>point (21)</b> of Article 2 of [Directive establishing the European Electronic Communications Code];	(b) the definitions of ‘electronic communications network’, ‘electronic communications service’, ‘interpersonal communications service’, ‘number-based interpersonal communications service’, ‘number-independent interpersonal communications service’, ‘end-user’ and ‘call’ in <del>points</del> <b>paragraphs</b> (1), (4), (5), (6), (7), (14) and (21) <b>31</b> respectively of Article 2 of [Directive <del>establishing the European Electronic Communications Code</del> ](EU) <b>2018/1972</b> ;	

AM 52

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 4(1), point (c)				
85	<p>(c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC<sup>1</sup>.</p> <p>1. Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20–26).</p>		<p>(c) the definition of 'terminal equipment' in <del>point (1)</del> of Article <del>1(1)</del> of Commission Directive 2008/63/EC<sup>1</sup>;</p> <p><del>1. Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20–26).</del></p>	Keine inhaltliche Änderung
Article 4(1), point (d)				
85a			<b>(d) the definition of ‘information society service’ in point (b) of Article 1 (1) of Directive (EU) 2015/1535.</b>	
Article 4(2)				
86	<p>2. For the purposes of point (b) of paragraph 1, the definition of ‘interpersonal communications service’ shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.</p>	<p><i>2. For the purposes of point (b) of paragraph 1, the definition of ‘interpersonal communications service’ shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.</i></p> <p>AM 53 deleted</p>	<p>2. For the purposes of <del>point (b) of paragraph 1</del><b>this Regulation</b>, the definition of ‘interpersonal communications service’ <b>referred to in point (b) of paragraph 1</b> shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.</p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 4(2a)				
86a			2a. For the purposes of this Regulation, the definition of 'processing' referred to in Article 4 (2) of Regulation 2016/679 shall not be limited to processing of personal data.	
Article 4(3), introductory part				
87	3. In addition, for the purposes of this Regulation the following definitions shall apply:		3. In addition, for the purposes of this Regulation the following definitions shall apply:	
Article 4(3), point (-a)				
87a		<i>(-a) 'electronic communications network' means a transmission system, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit - and packet - switched including Internet) and mobile terrestrial networks, electricity</i>		(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;</i>  AM 54		
Article 4(3), point (-aa)				
87b		(-aa) <i>'electronic communications service' means a service provided via electronic communications networks, whether for remuneration or not, which encompasses one or more of the following: an 'internet access service' as defined in Article 2(2) or Regulation (EU) 2015/2120; an interpersonal communications service; a service consisting wholly or mainly in the conveyance of the signals, such as a transmission service used for the provision of a machine-to-machine service and for broadcasting, but excludes information conveyed as part of a broadcasting service to the public over an electronic communications network or service except to the extent that the information can be related to the identifiable end-user</i>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>receiving the information; it also includes services which are not publicly available, but provide access to a publicly available electronic communications network;</i></p> <p>AM 55</p>		
Article 4(3), point (-ab)				
87c		<p><i>(-ab) 'interpersonal communications service' means a service, whether provided for remuneration or not, that enables direct interpersonal and interactive exchange of information between a finite number of persons whereby the persons initiating or participating in the communication determine the recipient(s);</i></p> <p>AM 56</p>		
Article 4(3), point (-ac)				
87d		<p><i>(-ac) 'number-based interpersonal communications service' means an interpersonal communications service which connects to the public switched telephone network, either by means of assigned numbering resources, i.e. number or numbers in national or international</i></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;</i> AM 57		
Article 4(3), point (-ad)				
87e		<i>(-ad) 'number-independent interpersonal communications service' means an interpersonal communications service which does not connect with the public switched telephone network, either by means of assigned numbering resources, i.e. a number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;</i> AM 58		
Article 4(3), point (-ae)				
87f		<i>(-ae) 'end-user' means a legal entity or a natural person using or requesting a publicly available electronic communications service;</i>		(a) "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 59		service;
Article 4(3), point (-af)				
87g		<p><i>(-af) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;</i></p> <p>AM 60</p>		
Article 4(3), point (a)				
88	(a) 'electronic communications data' means electronic communications content and electronic communications metadata;		(a) 'electronic communications data' means electronic communications content and electronic communications metadata;	
Article 4(3), point (b)				
89	(b) 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;	(b) 'electronic communications content' means the content <b><i>transmitted, distributed or</i></b> exchanged by means of electronic communications services, such as text, voice, videos, images, and sound. <b><i>Where metadata of other electronic communications services or protocols are transmitted, distributed or exchanged by using</i></b>	(b) 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>the respective service, they shall be considered electronic communications content for the respective service;</i>  AM 61		
Article 4(3), point (c)				
90	(c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;	(c) ‘electronic communications metadata’ means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content ; including data used to trace and identify the source and destination of a communication, data on the location of the <del>device generated</del> <b>terminal equipment processed</b> in the context of providing electronic communications services, and the date, time, duration and the type of communication;  AM 62	(c) ‘electronic communications metadata’ means data processed <del>in an</del> <b>by means of</b> electronic communications <del>networks</del> <b>services</b> for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;	(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;  (c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;
Article 4(3), point (d)				
91	(d) ‘publicly available directory’ means a directory of end-users of electronic communications services, whether in printed or electronic		(d) ‘publicly available directory’ means a directory of end-users of <del>electronic</del> <b>number-based interpersonal</b> communications	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service;		services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service <b>and the main function of which is to enable identification of such end-users;</b>	
Article 4(3), point (e)				
92	(e) 'electronic mail' means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;		(e) 'electronic <del>mail</del> <b>message</b> ' means any <del>electronic</del> message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient, <b>including e-mail, SMS, MMS and functionally equivalent applications and techniques;</b>	(h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
Article 4(3), point (f)				
93	(f) 'direct marketing communications' means any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or	(f) 'direct marketing communications' means any form of advertising, whether <i>in</i> written, <b>oral or video format, sent, served or presented</b> <del>or oral, sent</del> to one or more identified or identifiable end-users of electronic communications services, including the use of	(f) 'direct marketing communications' means any form of advertising, whether written or oral, sent <b>via a publicly available electronic communications service directly</b> to one or more <del>identified or identifiable end-users of electronic communications services, including</del>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	without human interaction, electronic mail, SMS, etc.;	automated calling and <del>communication</del> <b>communications</b> systems with or without human interaction, electronic mail, SMS, <i>fax machines</i> etc.;	<b>specific end-users, including the placing of voice-to-voice calls</b> , the use of automated calling and communication systems with or without human interaction, electronic <del>mail, SMS,</del> <b>message</b> etc.;	
	Article 4(3), point (g)			
94	(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems;	(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and <del>communication</del> <b>communications</b> systems, <i>including calls made using automated calling and communications systems which connect the called person to an individual</i> ;	(g) ‘direct marketing voice-to-voice calls’ means live calls, which do not entail the use of automated calling systems and communication systems;	
	Article 4(3), point (h)			
95	(h) ‘automated calling and communication systems’ means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, including calls made using automated calling and	(h) ‘automated calling and <del>communication</del> <b>communications</b> systems’ means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, <del>including calls made using automated calling and</del>	(h) ‘automated calling and communication systems’ means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, including calls made using automated calling and	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	communication systems which connect the called person to an individual.	<del>communication systems which connect the called person to an individual.</del> <a href="#">AM 65</a>	communication systems which connect the called person to an individual;	
Article 4(3), point (i)				
95a			(i) 'direct marketing calls' means direct marketing voice-to-voice calls and calls made via automated calling and communication systems for the purpose of direct marketing.	
Article 4(3), point (j)				
95b			(j) 'location data' means data processed by means of an electronic communications network or service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;	
Article 4a				
95c			Article 4a  Consent  <a href="#">See Lines 126-129</a>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
CHAPTER II				
96	CHAPTER II PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT	CHAPTER II PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL <del>AND LEGAL</del> PERSONS AND OF INFORMATION <del>STORED</del> <del>INPROCESSED BY AND</del> <b>RELATED TO</b> THEIR TERMINAL EQUIPMENT  AM 66	CHAPTER II PROTECTION OF ELECTRONIC COMMUNICATIONS OF <del>NATURAL AND LEGAL</del> <del>PERSONS AND OF</del> <del>INFORMATION STORED IN</del> <b>END-USERS AND OF THE</b> <b>INTEGRITY OF THEIR</b> TERMINAL EQUIPMENT	
Article 5				
97	Article 5 Confidentiality of electronic communications data	Article 5 Confidentiality of electronic communications <del>data</del>  AM 67	Article 5 Confidentiality of electronic communications data	
Article 5 (1)				
98	Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or	<b>1.</b> Electronic communications <del>data</del> shall be confidential. Any interference, with electronic communications <del>data</del> , such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or <b>any</b>	Electronic communications data shall be confidential. Any interference with electronic communications data, <del>such as</del> <b>by including</b> listening, tapping, storing, monitoring, scanning or other kinds of interception,	1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular,

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	processing of electronic communications <del>data</del> , by persons other than the end-users, shall be prohibited, <del>except when permitted by this Regulation.</del> AM 68	surveillance <del>or</del> and processing of electronic communications data, by <del>persons</del> <b>anyone</b> other than the end-users <b>concerned</b> , shall be prohibited, except when permitted by this Regulation.	they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.
Article 5 (1a)				
98a		<b><i>1a Confidentiality of electronic communications shall also apply to data related to or processed by terminal equipment.</i></b> AM 69		
Article 6				
99	Article 6 Permitted processing of electronic communications data	Article 6 <del>Permitted</del> <b><i>Lawful</i></b> processing of electronic communications data AM 70	Article 6 Permitted processing of electronic communications data	
Article 6(1), introductory part				
100				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	1. Providers of electronic communications networks and services may process electronic communications data if:	1. Providers of electronic communications networks and services may process electronic communications data <i>only if it is technically necessary to achieve the transmission of the communication, for the duration necessary for that purpose.</i>  AM 71	1. Providers of electronic communications networks and services <del>may</del> <b>shall be permitted to</b> process electronic communications data <b>only</b> if:	
Article 6(1), point (a)				
101	(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or	(a) <del>it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or</del>  AM 71 deleted	(a) it is necessary to <del>achieve the transmission of the</del> <b>provide an electronic</b> communication, <del>for the duration necessary for that purpose</del> <b>service; or</b>	
Article 6(1), point (b)				
102	(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.	(b) <del>it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.</del>  AM 71 deleted	(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults <del>and/or, errors,</del> <b>security risks or attacks on</b> <del>in the transmission of</del> electronic communications, <del>for the duration necessary for that purpose.</del> <b>networks and services;</b>	
Article 6(1), point (c)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
102a			(c) it is necessary to detect or prevent security risks or attacks on end-users' terminal equipment;	
Article 6(1), point (d)				
102b			(d) it is necessary for compliance with a legal obligation to which the provider is subject laid down by Union or Member State law, which respects the essence of the fundamental rights and freedoms and is 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, and the safeguarding against and the prevention of threats to public security.	
Article 6(2)				
102c			2 Electronic communications data shall only be permitted to be processed for the duration necessary for the specified purpose or purposes according to Articles 6 to 6c and if the specified purpose or purposes cannot be fulfilled by	(Article 5) 2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			processing information that is made anonymous.	transaction or of any other business communication.
Article 6(3)				
102d			3 A third party acting on behalf of a provider of electronic communications network or services may be permitted to process electronic communications data in accordance with Articles 6 to 6c provided that the conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.	
Article 6(1a)				
102e		<i>1a. Providers of electronic communications networks and services or other parties acting on behalf of the provider or the end-user may process electronic communications data only if it is technically necessary to maintain or restore the availability, integrity, confidentiality and security of the respective electronic communications network or services, or to detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.</i>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 72		
Article 6(2)				
103	2. Providers of electronic communications services may process electronic communications metadata if:	2. Providers of electronic communications services <i>and networks</i> may process electronic communications metadata <i>only</i> if: AM 73	2. <b>Without prejudice to Article (6) 1</b> , providers of electronic communications <b>networks and</b> services <del>may</del> <b>shall be permitted to</b> process electronic communications metadata <b>only</b> if: Mandate Art 6b(1)	
Article 6(2), point (a)				
104	(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 <sup>1</sup> for the duration necessary for that purpose; or  1. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).	(a) it is <i>strictly</i> necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 <sup>1</sup> for the duration <i>technically</i> necessary for that purpose; or  1. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).	(a) it is necessary <b>for the purposes of network management or network optimisation, or</b> to meet <del>mandatory</del> <b>technical</b> quality of service requirements pursuant to <del>[Directive establishing the European Electronic Communications Code]</del> <b>(EU) 2018/1972</b> or Regulation (EU) 2015/2120 <sup>1</sup> <del>for the duration necessary for that purpose</del> <b>2015/2120<sup>2</sup>; or</b>  1. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 74	Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1-18).  Mandate Art 6b(1)(a)	
Article 6(2), point (b)				
105	(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or	(b) it is <b>strictly</b> necessary for billing, <del>calculating</del> <b>determining</b> interconnection payments, detecting or stopping fraudulent, <del>or abusive</del> use of, or subscription to, electronic communications services; or  AM 75	(b) it is necessary for <b>the performance of an electronic communications service contract to which the end-user is party, or if necessary</b> for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or	
Article 6(2), point (c)				
106	(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.	(c) <del>the user</del> <del>the end-user</del> concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such <del>end-users</del> <b>users</b> , provided that the purpose or purposes concerned could not be fulfilled <del>by</del> <b>without the</b> processing <del>information that is made anonymous</del> <b>of such metadata</b> .  AM 76	(c) the end-user concerned has given <del>his or her</del> consent to the processing of <del>his or her</del> communications metadata for one or more specified purposes, <del>including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made</del> <b>anonymous; or</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 6(2), point (ca)				
106a			(d) it is necessary in order to protect the vital interest of a natural person; or	
Article 6(2), point (cb), introductory part				
106b			(e) in relation to metadata that constitute location data, it is necessary for scientific or historical research purposes or statistical purposes, provided that:	
Article 6(2), point (cb)(i)				
106c			i such data is pseudonymised;	
Article 6(2), point (cb)(ii)				
106d			ii the processing could not be carried out by processing information that is made anonymous, and the location data is erased or made anonymous when it is no longer needed to fulfil the purpose; and	
Article 6(2), point (cb)(iii)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
106e			iii the location data is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.	
Article 6(2), point (cc)				
106f			(f) in relation to metadata other than location data, it is necessary for scientific or historical research purposes or statistical purposes, provided that such processing is in accordance with Union or Member State law and subject to appropriate safeguards, including encryption and pseudonymisation, to protect fundamental rights and the interest of the end-users and is in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.	
Article 6(2), point (cd)				
106g			2a Data processed under point e and f of paragraph 1 of this article may also be used for the development, production and dissemination of official national and European statistics to the extent necessary for this purpose	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			and in accordance, respectively, with national or Union law.	
Article 6(2), point (ce)				
106h			2 Without prejudice to Article 6 (3), electronic communications metadata processed pursuant to paragraph 1 (e) shall not be shared by the provider with any third party unless it has been made anonymous.	
Article 6(2a)				
106i		2a. For the purposes of point (c) of paragraph 2, where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, Articles 35 and 36 of Regulation (EU) 2016/679 shall apply.  AM 77		
Article 6(3), introductory part				
107	3. Providers of the electronic		3. Without prejudice to Article (6)	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	communications services may process electronic communications content only:		<b>1</b> , providers of the electronic communications <b>networks and services</b> <del>may</del> <b>shall be permitted to</b> process electronic communications content only:  Mandate Article 6a(1)	
Article 6(3), point (a)				
108	(a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or	(a) for the sole purpose of the provision of a specific service <del>to an end-user</del> <b>requested by the user</b> , if the <del>end-user or end-users</del> <b>user</b> concerned <del>have</del> <b>has</b> given <b>his or her</b> <del>their</del> consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content <b>by the provider; or</b> <del>or</del>  AM 78	Deleted	3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 6(3), point (aa)				
108a			<p><b>(a) for the purpose of the provision of a service requested by an end-user for purely individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interests of another person concerned; or</b></p> <p>Mandate Art 6a(1)(a)</p>	
Article 6(3), point (b)				
109	<p>(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.</p>	<p>(b) if all <del>end-users</del><b>users</b> concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.</p> <p>AM 79</p>	<p>(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes <del>that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.</del></p> <p>Mandate Art 6a(1)(b)</p>	
Article 6(3), point (ba)				
109a				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<p><b>2 Prior to the processing in accordance with point (b) of paragraph 1 the provider shall carry out a data protection impact assessment of the impact of the envisaged processing operations on the protection of electronic communications data and consult the supervisory authority if necessary pursuant to Article 36 (1) of Regulation (EU) 2016/679. Article 36 (2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.</b></p> <p>Mandate Art 6a(2)</p>	
Article 6(3a)				
109b		<p><i>3a. The provider of the electronic communications service may process electronic communications data solely for the provision of an explicitly requested service, for purely individual usage, only for the duration necessary for that purpose and without the consent of all users only where such requested processing does not adversely affect the fundamental rights and interests of another user or users.</i></p> <p>AM 80</p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 6a				
109c			<b>Article 6a</b> <b>Permitted processing of electronic communications content</b> <b>[previous art. 6(3)]</b> <a href="#">See Lines 107-109b</a>	
Article 6b				
109d			<b>Article 6b</b> <b>Permitted processing of electronic communications metadata</b> <b>[previous art 6(2)]</b> <a href="#">See Lines 103-106i</a>	
Article 6c				
109e			<b>Article 6c</b> <b>Compatible processing of electronic communications metadata</b> <b>[Previous art 6(2a)]</b>	
Article 6c(1)				
109f			<b>1. Where the processing for a purpose other than that for which the electronic communications metadata have been collected under paragraph 1 of Articles 6</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			and 6b is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11, the provider of electronic communications networks and services shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications metadata are initially collected, take into account, inter alia:	
Article 6c(1), point (a)				
109g			(a) any link between the purposes for which the electronic communications metadata have been collected and the purposes of the intended further processing;	
Article 6c(1), point (b)				
109h			(b) the context in which the electronic communications metadata have been collected, in particular regarding the relationship between end-users	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			concerned and the provider;	
Article 6c(1), point (c)				
109i			(c) the nature of the electronic communications metadata as well as the modalities of the intended further processing, in particular where such data or the intended further processing could reveal categories of data, pursuant to Articles 9 or 10 of Regulation (EU) 2016/679;	
Article 6c(1), point (d)				
109j			(d) the possible consequences of the intended further processing for end-users;	
Article 6c(1), point (e)				
109k			(e) the existence of appropriate safeguards, such as encryption and pseudonymisation.	
Article 6c(2),				
109l			2. Such processing, if considered compatible, may only take place, provided that:	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 6c(2),, point (a)				
109m			(a) the processing could not be carried out by processing information that is made anonymous, and electronic communications metadata is erased or made anonymous as soon as it is no longer needed to fulfil the purpose, and	
Article 6c(2),, point (b)				
109n			(b) the processing is limited to electronic communications metadata that is pseudonymised, and	
Article 6c(2),, point (c)				
109o			(c) the electronic communications metadata is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user, which produces legal effects concerning him or her or similarly significantly affects him or her.	
Article 6c(3)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
109p			3. For the purposes of paragraph 1 of this Article, the providers of electronic communications networks and services shall not, without prejudice to Article 6 (3), share such data with any third parties, unless it is made anonymous.	
Article 7				
110	Article 7 Storage and erasure of electronic communications data	Article 7 Storage and erasure of electronic communications data	Article 7 Storage and erasure of electronic communications data	Article 6
Article 7(1)				
111	1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.	1. Without prejudice to <del>point (b) of Article 6(1) and points (a) and (b) of Article 6(3),</del> the provider of the electronic communications service shall erase electronic communications content, <b>when it is no longer necessary for the provision of such service, as requested or make that data anonymous after receipt of electronic communication content</b> by the <del>intended recipient or recipients</del> user. Such data may be recorded or stored by the <del>end-users</del> users or by a third party	1. <del>Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3),</del> The provider of the electronic communications service shall erase electronic communications content or make that data anonymous <del>after receipt of electronic communication content by the intended recipient or recipients.</del> Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679 <b>when it is no longer</b>	1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		entrusted by them to record, store or otherwise process such data. <i>The user may process the data</i> in accordance with Regulation (EU) 2016/679.  AM 81	necessary for the purpose of processing in accordance to article 6 (1) and 6a (1).	
Article 7(2)				
112	2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.	2. Without prejudice to <del>point (b) of Article 6(1)</del> <b>6(1b)</b> and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer <del>needed</del> <b>necessary</b> for the <del>purpose of the transmission of a communication</del> <b>provision of such service, as requested by the user.</b>  AM 82	2. Without prejudice to <b>points (b), (c) and (d) of Article 6 (1), points (c), (d), (e), (f), point (b)() of Article <del>6(1)</del><b>6b, Article 6c</b> and points <del>(a) and (e)(b) to (g) of Article 6(2)</del><b>,8 (1)</b> the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of <del>the transmission of</del><b>providing an electronic communication service.</b></b>	3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.  4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
				in paragraph 3.
Article 7(3)				
113	3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.	3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), <del>the relevant</del> <b>strictly necessary</b> metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.  AM 83	3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2) <b>6b (1)</b> , the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged, or a payment may be pursued in accordance with national law.	2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.
Article 7(4)				
113a			<b>4 Union or Member state law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			prevention of threats to public security, for a limited period. The duration of the retention may be extended if threats to public security of the Union or of a Member State persists.	
Article 8				
114	Article 8 Protection of information stored in and related to end-users' terminal equipment	Article 8 Protection of information <i>transmitted to</i> , stored in and related to <del>end-users</del> <i>processed by and collected from users</i> ' terminal equipment  AM 84	Article 8 Protection of <del>information stored in and related to end-users'</del> terminal equipment <b>information</b>	
Article 8(1), introductory part				
115	1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:	1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the <del>end-user</del> <i>user</i> concerned shall be prohibited, except on the following grounds:  AM 85	1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:	
Article 8(1), point (a)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
116	(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or	(a) it is <b>strictly</b> necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or  AM 86	(a) it is necessary for the sole purpose of <del>carrying out the transmission of</del> <b>providing</b> an electronic communication <del>over an electronic communications network</del> <b>service</b> ; or	
Article 8(1), point (b)				
117	(b) the end-user has given his or her consent; or	(b) the <del>end-user</del> <b>user</b> has given his or her <b>specific</b> consent; or  AM 87	(b) the end-user has given <del>his or her</del> consent; or	
Article 8(1), point (c)				
118	(c) it is necessary for providing an information society service requested by the end-user; or	(c) it is <b>strictly technically</b> necessary for providing an information society service <b>specifically</b> requested by the <del>end-user</del> <b>user</b> ; or  AM 88	(c) it is <b>strictly</b> necessary for providing <del>an information society service</del> <b>a service specifically</b> requested by the end-user; or	
Article 8(1), point (d)				
119	(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-	(d) if it is <b>technically</b> necessary for <del>web audience measuring</del> <b>measuring the reach of an information society service requested by the user</b> , provided that such measurement is	(d) <del>if it is necessary for web</del> <b>the sole purpose of</b> audience measuring, provided that such measurement is carried out by the provider of the <del>information society</del> service	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	user.	<p>carried out by the provider, <i>or on behalf of the provider, or by a web analytics agency acting in the public interest including for scientific purpose; that the data is aggregated and the user is given a possibility to object; and further provided that no personal data is made accessible to any third party and that such measurement does not adversely affect the fundamental rights of the user; Where audience measuring takes place on behalf of an</i> information society service <del>requested by the end-user</del> <i>provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers; or</i></p> <p>AM 89</p>	<p>requested by the end-user, <i>or by a third party, or by third parties jointly on behalf of or jointly with provider of the service requested provided that, where applicable, the conditions laid down in Articles 26 or 28 of Regulation (EU) 2016/679 are met; or</i></p>	
Article 8(1), point (da)				
119a		<p><i>(da) it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:</i></p> <p>AM 90</p>	<p><i>(da) it is necessary to maintain or restore the security of information society services or terminal equipment of the end-user, prevent fraud or prevent or detect technical faults for the duration necessary for that purpose; or</i></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 8(1), point (da)(i)				
119b		<p><i>(i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;</i></p> <p>AM 90</p>		
Article 8(1), point (da)(ii)				
119c		<p><i>(ii) the user is informed in advance each time an update is being installed; and</i></p> <p>AM 90</p>		
Article 8(1), point (da)(iii)				
119d		<p><i>(iii) the user has the possibility to postpone or turn off the automatic installation of these updates;</i></p> <p>AM 90</p>		
Article 8(1), point (db), introductory part				
119e		<p><i>(db) in the context of employment relationships, it is strictly technically necessary for the execution of an employee's task, where:</i></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 91		
Article 8(1), point (db)(i)				
119f		<i>(i) the employer provides and/or is the user of the terminal equipment;</i> AM 91		
Article 8(1), point (db)(ii)				
119g		<i>(ii) the employee is the user of the terminal equipment; and</i> AM 91		
Article 8(1), point (db)(iii)				
119h		<i>(iii) it is not further used for monitoring the employee.</i> AM 91		
Article 8(1), point (e)				
119i			<b>(e) it is necessary for a software update provided that:</b>	
Article 8(1), point (e)(i)				
119j			<b>i such update is necessary for</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			security reasons and does not in any way change the privacy settings chosen by the end-user,	
Article 8(1), point (e)(ii)				
119k			ii the end-user is informed in advance each time an update is being installed, and	
Article 8(1), point (e)(iii)				
119l			iii the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or	
Article 8(1), point (f)				
119m			(f) it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3).	
Article 8(1), point (g)				
119n			(g) where the processing for	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			purpose other than that for which the information has been collected under this paragraph is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 the person using processing and storage capabilities or collecting information processed by or emitted by or stored in the end-users' terminal equipment shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:	
Article 8(1), point (g)(i)				
119o			i any link between the purposes for which the processing and storage capabilities have been used or the information have been collected and the purposes of the intended further processing;	
Article 8(1), point (g)(ii)				
119p				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			ii the context in which the processing and storage capabilities have been used or the information have been collected, in particular regarding the relationship between end-users concerned and the provider;	
Article 8(1), point (g)(iii)				
119q			iii the nature the processing and storage capabilities or of the collecting of information as well as the modalities of the intended further processing, in particular where such intended further processing could reveal categories of data, pursuant to Article 9 or 10 of Regulation (EU) 2016/679;	
Article 8(1), point (g)(iv)				
119r			iv the possible consequences of the intended further processing for end-users;	
Article 8(1), point (g)(v)				
119s			v the existence of appropriate safeguards, such as encryption and pseudonymisation.	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 8(1), point (h)				
119t			<b>(h) Such further processing in accordance with paragraph 1 (g), if considered compatible, may only take place, provided that:</b>	
Article 8(1), point (h)(i)				
119u			<b>i the information is erased or made anonymous as soon as it is no longer needed to fulfil the purpose,</b>	
Article 8(1), point (h)(ii)				
119v			<b>ii the processing is limited to information that is pseudonymised, and</b>	
Article 8(1), point (h)(iii)				
119w			<b>iii the information is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.</b>	
Article 8(1), point (i)				
119x			<b>(i) For the purposes of paragraph 1 (g) and (h), data shall not be</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			shared with any third parties unless the conditions laid down in Article 28 of Regulation (EU) 2016/697 are met, or data is made anonymous.	
Article 8(1a)				
119y		<p><i>1a. No user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal information and/or the use of processing or storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality.</i></p> <p>AM 92</p>		
Article 8(2), first subparagraph, introductory part				
120	2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:	<p>2. <del>The processing</del><del>The collection</del> of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:</p> <p>AM 93</p>	2. The collection of information emitted by terminal equipment of <b>the end-user</b> to enable it to connect to another device and, or to network equipment shall be prohibited, except <del>if</del> <b>on the following grounds:</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 8(2), first subparagraph, point (a)				
121	(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or	(a) <del>#</del> is done exclusively in order to, for the time necessary for, and for the <b>sole</b> purpose of establishing a connection <b><i>requested by the user</i></b> ; or <a href="#">AM 94</a>	(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing <b>or maintaining</b> a connection; or	
Article 8(2), first subparagraph, point (aa)				
121a		<b><i>(aa) the user has been informed and has given consent; or</i></b> <a href="#">AM 95</a>	<b>(b) the end-user has given consent; or</b>	
Article 8(2), first subparagraph, point (ab)				
121b		<b><i>(ab) the risks are mitigated.</i></b> <a href="#">AM 96</a>		
Article 8(2)(c)				
121c			<b>(c) it is necessary for the purpose of statistical purposes that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose,</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 8(2)(d)				
121d			(d) it is necessary for providing a service requested by the end-user.	
Article 8(2), first subparagraph, point (b)				
122	(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.	<del>(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.</del> AM 97 deleted	<del>(b)</del> <b>2a</b> For the purpose of paragraph 2 points (b) and (c), a clear and prominent notice shall be is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.	
Article 8(2), second subparagraph				
123	The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	<del>The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.</del> AM 98 deleted	<b>2b</b> For the purpose of paragraph 2 points (b) and (c), the collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 8(2a), introductory part				
123a		<p><i>2a. For the purpose of points (d) of paragraph 1 and (ab) of paragraph 2, the following controls shall be implemented to mitigate the risks:</i></p> <p>AM 99</p>		
Article 8(2a), point (a)				
123b		<p><i>(a) the purpose of the data collection from the terminal equipment shall be restricted to mere statistical counting; and</i></p> <p>AM 99</p>		
Article 8(2a), point (b)				
123c		<p><i>(b) the processing shall be limited in time and space to the extent strictly necessary for this purpose; and</i></p> <p>AM 99</p>		
Article 8(2a), point (c)				
123d		<p><i>(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and</i></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 99		
Article 8(2a), point (d)				
123e		<p><i>(d) the users shall be given effective possibilities to object that do not affect the functionality of the terminal equipment.</i></p> <p>AM 99</p>		
Article 8(2b)				
123f		<p><i>2b. The information referred to in points (aa) and (ab) of paragraph 2 shall be conveyed in a clear and prominent notice setting out, at the least, details of how the information will be collected, the purpose of processing, the person responsible for it and other information required under Article 13 of Regulation (EU) 2016/679, where personal data are collected. The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679.</i></p> <p>AM 100</p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 8(3)				
124	3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	3. The information to be provided pursuant to <del>point (b) of</del> paragraph <del>22b</del> may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.  AM 101	3. The information to be provided pursuant to <del>point (b) of</del> paragraph <del>22a</del> may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	
Article 8(4)				
125	4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.		4. The Commission shall be empowered to adopt delegated acts in accordance with Article <del>27</del> <b>25</b> determining the information to be presented by the standardized icon and the procedures for providing standardized icons.	
Article 9				
126	Article 9 Consent	Article 9 Consent	Article 9 <b>Article 4a</b> Consent  Article 4a in the Council Mandate	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 9(1)				
127	1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.	1. The definition of and conditions for consent provided for <del>under Articles 4(11) and 7 of</del> Regulation (EU) 2016/679/EU shall apply.  AM 102	1. The <del>definition of and conditions</del> <b>provisions</b> for consent provided for under <del>Articles 4(11) and 7 of</del> <b>Regulation (EU) 2016/679/EU shall apply to natural persons and, mutatis mutandis, to legal persons.</b>	(Article 2) (f) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;
Article 9(1a)				
127a			<b>1a. Paragraph 1 is without prejudice to national legislation on determining the persons who are authorised to represent a legal person in any dealings with third parties or in legal proceedings.</b>	
Article 9(2)				
128	2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.	2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed <i>or withdrawn</i> by using <b>technical specifications for electronic communications services or information society services which allow for specific consent for specific purposes and with regard to specific service providers actively</b>	2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article <del>8(1)</del> <b>8 (1)</b> , consent may be expressed by using the appropriate <b>placed on the market permitting electronic communications, including the retrieval and presentation of information on</b> <del>application enabling access to the</del>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>selected by the user in each case, pursuant to paragraph 1. When <del>such</del>the appropriate technical settings of aspecifications are used by the user's terminal equipment or the software application enabling access to the internetrunning on it, they may signal the user's choice based on previous active selections by him or her. These signals shall be binding on, and enforceable against, any other party.</i></p> <p>AM 103</p>	internet.	
Article 9(2a)				
128a			<p><b>2a. Consent directly expressed by an end-user in accordance with Paragraph (2) shall prevail over software settings. Any consent requested and given by an end-user to a service shall be directly implemented, without any further delay, by the applications of the end user's terminal, including where the storage of information or the access of information already stored in the end-user's terminal equipment is permitted.</b></p> <p>Mandate Art 4a(2aa)</p>	
Article 9(2b)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
128b			<p>2b. As far as the provider is not able to identify a data subject, the technical protocol showing that consent was given from the terminal equipment shall be sufficient to demonstrate the consent of the end-user according Article 8 (1) (b).</p> <p>Mandate Art 4a(2a)</p>	
Article 9(3)				
129	<p>3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.</p>	<p>3. <del>End-users</del><b>Users</b> who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3), <b>point (b) of Article 8(1) and point (aa) of Article 8(2)</b> shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 <del>and be reminded of this possibility at periodic intervals of 6 months,</del> as long as the processing continues.</p> <p>AM 104</p>	<p>3. End-users who have consented to the processing of electronic communications data <del>as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given in accordance with this Regulation shall be reminded of</del> the possibility to withdraw their consent at <del>any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of</del> this possibility at periodic intervals of 6 months, as long as the processing continues<b>periodic intervals of [no longer than 12 months], as long as the processing continues, unless the end-user requests not to receive such reminders.</b></p>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 9(3a)				
129a		<p><i>3a. Any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communication, in particular their rights to privacy and the protection of personal data.</i></p> <p>AM 105</p>		
Article 10				
130	Article 10 Information and options for privacy settings to be provided	Article 10 Information and options for privacy settings to be provided	Deleted	
Article 10(1)				
131	1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.	<p>1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall <del>offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.:</del></p> <p>AM 106</p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 10(1), point (a)				
131a		<p><i>(a) by default, have privacy protective settings activated to prevent other parties from transmitting to or storing information on the terminal equipment of a user and from processing information already stored on or collected from that equipment, except for the purposes laid down by Article 8(1), points (a) and (c);</i></p> <p>AM 107</p>		
Article 10(1), point (b)				
131b		<p><i>(b) upon installation, inform and offer the user the possibility to change or confirm the privacy settings options defined in point (a) by requiring the user's consent to a setting and offer the option to prevent other parties from processing information transmitted to, already stored on or collected from the terminal equipment for the purposes laid down by Article 8(1) points (a), (c), (d) and (da);</i></p> <p>AM 108</p>		
Article 10(1), point (c)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
131c		<p><i>(c) offer the user the possibility to express specific consent through the settings after the installation of the software.</i></p> <p>AM 109</p>		
Article 10(1), subparagraph 1 (new)				
131d		<p><i>Before the first use of the software, the software shall inform the user about the privacy settings and the available granular setting options according to the information society service accessed. These settings shall be easily accessible during the use of the software and presented in a manner that gives the user the possibility for making an informed decision.</i></p> <p>AM 110</p>		
Article 10(1a), introductory part				
131e		<p><i>1a. For the purpose of:</i></p> <p>AM 111</p>		
Article 10(1a), point (a)				
131f				


	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>(a) points (a) and (b) of paragraph 1,</i> <a href="#">AM 112</a>		
Article 10(1a), point (b)				
131g		<i>(b) giving or withdrawing consent pursuant to Article 9(2) of this Regulation, and</i> <a href="#">AM 113</a>		
Article 10(1a), point (c)				
131h		<i>(c) objecting to the processing of personal data pursuant to Article 21(5) of Regulation (EU) 2017/679,</i> <a href="#">AM 114</a>		
Article 10(1a), subparagraph 1 (new)				
131i		<i>the settings shall lead to a signal based on technical specifications which is sent to the other parties to inform them about the user's intentions with regard to consent or objection. This signal shall be legally valid and be binding on, and enforceable against, any other party.</i>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 115		
Article 10(1b))				
131j		<p><i>1b. In accordance with Article 9 paragraph 2, such software shall ensure that a specific information society service may allow the user to express specific consent. A specific consent given by a user pursuant to point (b) of Article 8(1) shall prevail over the existing privacy settings for that particular information society service. Without prejudice to paragraph 1, where a specified technology has been authorised by the data protection board for the purposes of point (b) of Article 8(1), consent may be expressed or withdrawn at any time both from within the terminal equipment and by using procedures provided by the specific information society service.</i></p> <p>AM 116</p>		
Article 10(2)				
132	2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.	<p><del>2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.</del></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 117 deleted		
Article 10(3)				
133	3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.	3. In the case of software which has already been installed on <del>25 May 2018</del> <del>[xx.xx.xxxx]</del> , the requirements under paragraphs 1, <del>1a and 1b and 2</del> shall be complied with at the time of the first update of the software, but no later than <del>25 August 2018</del> <i>six months after [the date of entry into force of this Regulation]</i> .  AM 118		
Article 11				
134	Article 11 Restrictions	Article 11 <i>Restrictions</i>  AM 119 deleted	Article 11 Restrictions	
Article 11(1)				
135	1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary,	1. <del>Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms</del>	1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary,	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.	<del>and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.</del> AM 119 deleted	appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) <b>23(1) (c) to (e), (i) and (j)</b> of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.	
Article 11(1a)				
135a			<b>1a. Article 23 (2) of Regulation (EU) 2016/679 shall apply to any legislative measures referred to in paragraph 1.</b>	
Article 11(2)				
136	2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal	<del>2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the</del>	2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	justification invoked and their response.	<del>legal justification invoked and their response.</del> AM 119 deleted	justification invoked and their response.	
Article 11a				
136a		<b>Article 11a</b> <b>Restrictions on the rights of the user</b>  AM 120		
Article 11a(1)				
136b		<b>1. Union or Member State law to which the provider is subject may restrict by way of a legislative measure the scope of the obligations and principles relating to processing of electronic communications data provided for in Articles 6, 7 and 8 of this Regulation in so far as its provisions correspond to the rights and obligations provided for in Regulation (EU) 2016/679, when such a restriction fully respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to</b>		Application of certain provisions of Directive 95/46/EC 1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>in Article 23(1)(a) to (d) of Regulation (EU) 2016/679.</i> AM 120		95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.
Article 11a(2)				
136c		2. <i>In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, pursuant to Article 23(2) of Regulation (EU) 2016/679.</i> AM 120		
Article 11b				
136d		Article 11b <i>Restrictions on confidentiality of communications</i> AM 121		
Article 11b(1), introductory part				
136e				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>1. Union or Member State law may restrict by way of a legislative measure the scope of the rights provided for in Article 5 where such a restriction fully respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the following general public interests:</i></p> <p>AM 121</p>		
Article 11b(1), point (a)				
136f		<p><i>(a) national security;</i></p> <p>AM 121</p>		
Article 11b(1), point (b)				
136g		<p><i>(b) defence</i></p> <p>AM 121</p>		
Article 11b(1), point (c)				
136h		<p><i>(c) public security;</i></p> <p>AM 121</p>		
Article 11b(1), point (d)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
136i		<p><i>(d) the prevention, investigation, detection or prosecution of serious criminal offences, unauthorised use of electronic communication systems or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.</i></p> <p>AM 121</p>		
Article 11b(2)				
136j		<p><i>2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, pursuant to Article 23(2) of Regulation (EU) 2016/679.</i></p> <p>AM 121</p>		
Article 11c				
136k		<p><i>Article 11c Documentation and reporting of restrictions</i></p> <p>AM 122</p>		
Article 11c(1), introductory part				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
136l		<p><i>1. Providers of electronic communications services shall keep documentation about requests made by competent authorities to access communications content or metadata pursuant to Article 11b(2). This documentation shall include for each request:</i></p> <p>AM 122</p>		<p>2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.</p>
Article 11c(1), point (a)				
136m		<p><i>(a) the in-house staff member who handled the request;</i></p> <p>AM 122</p>		
Article 11c(1), point (b)				
136n		<p><i>(b) the identity of the body making the request;</i></p> <p>AM 122</p>		
Article 11c(1), point (c)				
136o		<p><i>(c) the purpose for which the information was sought;</i></p> <p>AM 122</p>		
Article 11c(1), point (d)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
136p		<i>(d) the date and time of the request;</i> <a href="#">AM 122</a>		
Article 11c(1), point (e)				
136q		<i>(e) the legal basis and authority for the request, including the identity and status or function of the official submitting the request;</i> <a href="#">AM 122</a>		
Article 11c(1), point (f)				
136r		<i>(f) the judicial authorisation of the request;</i> <a href="#">AM 122</a>		
Article 11c(1), point (g)				
136s		<i>(g) (g) the number of users to whose data the request related</i> <a href="#">AM 122</a>		
Article 11c(1), point (h)				
136t		<i>(h) the data provided to the requesting authority; and</i>		3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 122		instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.
Article 11c(1), point (i)				
136u		(i) <i>the period covered by the data.</i> AM 122		
Article 11c(2), second subparagraph				
136v		<i>The documentation shall be made available to the competent supervisory authority upon request.</i>		
Article 11c(2), introductory part				
136w		<i>2. Providers of electronic communications services shall publish once per year a report with statistical information about data access requests by law enforcement authorities pursuant to Articles 11a and 11b. The report shall include, at least:</i> AM 122		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 11c(2), point (a)				
136x		<p><i>(a) the number of requests;</i></p> <p>AM 122</p>		
Article 11c(2), point (b)				
136y		<p><i>(b) the categories of purposes for the request;</i></p> <p>AM 122</p>		
Article 11c(2), point (c)				
136z		<p><i>(c) the categories of data requested;</i></p> <p>AM 122</p>		
Article 11c(2), point (d)				
136aa		<p><i>(d) the legal basis and authority for the request;</i></p> <p>AM 122</p>		
Article 11c(2), point (e)				
136ab		<p><i>(e) the number of users to whose data the request related;</i></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 122		
Article 11c(2), point (f)				
136ac		<i>(f) the period covered by the data;</i> AM 122		
Article 11c(2), point (g)				
136ad		<i>(g) the number of negative and positive responses to those requests.</i> AM 122		
Article 11c(3), introductory part				
136ae		<i>3. Member States' competent authorities shall publish once per year a report with statistical information per month about data access requests pursuant to Articles 11a and 11b, including requests that were not authorised by a judge, including, but not limited to, the following points:</i> AM 122		
Article 11c(3), point (a)				
136af		<i>(a) the number of requests;</i>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		AM 122		
Article 11c(3), point (b)				
136ag		<i>(b) the categories of purposes for the request;</i> AM 122		
Article 11c(3), point (c)				
136ah		<i>(c) the categories of data requested;</i> AM 122		
Article 11c(3), point (d)				
136ai		<i>(d) the legal basis and authority for the request;</i> AM 122		
Article 11c(3), point (e)				
136aj		<i>(e) the number of users to whose data the request related;</i> AM 122		
Article 11c(3), point (f)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
136ak		<i>(f) the period covered by the data;</i> AM 122		
Article 11c(3), point (g)				
136al		<i>(g) the number of negative and positive responses to those requests.</i> AM 122		
Article 11c(3), second subparagraph				
136am		<i>The reports shall also contain statistical information per month about any other restrictions pursuant to Articles 11a and 11b.</i>		
CHAPTER III				
137	CHAPTER III NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS	CHAPTER III NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS	CHAPTER III <del>NATURAL AND LEGAL PERSONS</del> <b>END-USERS'</b> RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS	
Article 12				
138	Article 12 Presentation and restriction of	Article 12 Presentation and restriction of	Article 12 Presentation and restriction of	(Article 8) Presentation and restriction of calling and connected

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	calling and connected line identification	calling and connected line identification	calling and connected line identification	line identification
Article 12(1), introductory part				
139	1. Where presentation of the calling and connected line identification is offered in accordance with Article [107] of the [Directive establishing the European Electronic Communication Code], the providers of publicly available number-based interpersonal communications services shall provide the following:		1. Where presentation of the calling and connected line identification is offered in accordance with Article [107 <del>115</del> ] of the [ <del>Directive establishing the European Electronic Communication Code</del> ](EU) <b>2018/1972</b> , the providers of publicly available number-based interpersonal communications services shall provide the following:	1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, <b>using a simple means and free of charge</b> , of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.
Article 12(1), point (a)				
140	(a) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis;		(a) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis;	2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, <b>using a simple means and free of charge for reasonable use of this function</b> , of preventing the presentation of the calling line identification of incoming calls.
Article 12(1), point (b)				
141	(b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;		(b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;	3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of
Article 12(1), point (c)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
142	(c) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user;		(c) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user;	rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.
Article 12(1), point (d)				
143	(d) the called end-user with the possibility of preventing the presentation of the connected line identification to the calling end-user.		(d) the called end-user with the possibility of preventing the presentation of the connected line identification to <b>which</b> the calling end-user <b>is connected</b> .	4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.
Article 12(2)				
144	2. The possibilities referred to in points (a), (b), (c) and (d) of paragraph 1 shall be provided to end-users by simple means and free of charge.		2. The possibilities referred to in <del>points (a), (b), (c) and (d)</del> of paragraph 1 shall be provided to end-users by simple means and free of charge.	
Article 12(3)				
145	3. Point (a) of paragraph 1 shall also apply with regard to calls to third countries originating in the Union. Points (b), (c) and (d) of paragraph 1		3. Point (a) of paragraph 1 shall also apply with regard to calls to third countries originating in the Union. Points (b), (c) and (d) of paragraph 1	5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	shall also apply to incoming calls originating in third countries.		shall also apply to incoming calls originating in third countries.	apply to incoming calls originating in third countries.
Article 12(4)				
146	4. Where presentation of calling or connected line identification is offered, providers of publicly available number-based interpersonal communications services shall provide information to the public regarding the options set out in points (a), (b), (c) and (d) of paragraph 1.		4. Where presentation of calling or connected line identification is offered, providers of <del>publicly available</del> number-based interpersonal communications services shall provide information to the public regarding the options set out in <del>points (a), (b), (c) and (d) of paragraph 1</del> <b>paragraph 1 and the exceptions set forth in Article 13.</b>	6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.
Article 13				
147	Article 13 Exceptions to presentation and restriction of calling and connected line identification	Article 13 Exceptions to presentation and restriction of calling and connected line identification	Article 13 Exceptions to presentation and restriction of calling and connected line identification <b>in relation to emergency communications</b>	Article 10 Exceptions
Article 13(1)				
148	1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based	1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based	1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where <del>a call is made to emergency services,</del> <b>emergency communications are made to emergency services,</b>	Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.	interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of <del>an end-user</del> <b>a user</b> for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.  AM 123	providers of <del>publicly available</del> number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.	may override: ... (b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.
Article 13(1a)				
148a			<b>1a. Regardless whether the called end-user rejects incoming calls where the presentation of the calling line identification has been prevented by the calling end-user, providers of number-based interpersonal communications services shall override this choice, where technically possible, when the calling end-user is an organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 13(2)				
149	2. Member States shall establish more specific provisions with regard to the establishment of procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of malicious or nuisance calls.	2. <del>Member States</del> <b>The Commission</b> shall <del>establish more specific provisions</del> <b>be empowered to adopt implementing measures in accordance with Article 26(1)</b> with regard to the establishment of procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where <del>end-users</del> <b>users</b> request the tracing of malicious or nuisance calls.  AM 124	Deleted	Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:  (a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;
Article 13(3)				
149a			<b>3. Notwithstanding Article 8(1), regardless of whether the end-user has prevented access to the terminal equipment's Global Navigation Satellite Systems (GNSS) capabilities or other types of terminal equipment based location data through the terminal equipment settings, when a call is made to emergency services, such</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			settings may not prevent access to such location data to determine and provide the calling end-user's location to an organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such calls.	
Article 14				
150	Article 14 Incoming call blocking	Article 14 Incoming call blocking	Article 14 <del>Incoming call blocking</del> <b>Blocking unwanted, malicious or nuisance calls</b>	Article 11 Automatic Call forwarding
Article 14, first paragraph, introductory part				
151	Providers of publicly available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge:	Providers of publicly available number-based interpersonal communications services <del>shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide</del> the called end-user with the following possibilities, free of charge:  AM 125	<b>1</b> Providers of publicly available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge: <b>malicious or nuisance calls by end-users.</b>	Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.
Article 14(1a)				
151a				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			<b>1a Member States shall establish more specific provisions with regard to the establishment of transparent procedures and the circumstances where providers of number-based interpersonal communication services shall override, or otherwise address, the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of unwanted, malicious or nuisance calls.</b>	
Article 14(2)				
151b			<b>2. Providers of number-based interpersonal communications services shall also provide the called end-user with the following possibilities, free of charge:</b>	
Article 14, first paragraph, point (a)				
152	(a) to block incoming calls from specific numbers or from anonymous sources;	(a) to block incoming calls from specific numbers, <i>or numbers having a specific code or prefix identifying the fact that the call is a marketing call referred to in Article 16(3)(b)</i> , or from anonymous sources;  <a href="#">AM 126</a>	(a) to block, <b>where technically feasible</b> , incoming calls from specific numbers or from anonymous sources <b>or from numbers using a specific code or prefix referred to in Article 16(3a); and</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 14, first paragraph, point (b)				
153	(b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.	(b) to stop automatic call forwarding by a third party to the <del>end-user</del> <b>user's</b> terminal equipment.  AM 127	(b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.	
Article 15				
154	Article 15 Publicly available directories	Article 15 Publicly available directories	Article 15 Publicly available directories	(Article 12) Directories of subscribers
Article 15(1)				
155	1. The providers of publicly available directories shall obtain the consent of end-users who are natural persons to include their personal data in the directory and, consequently, shall obtain consent from these end-users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.	1. <del>The providers of publicly available directories</del> <b>Without prejudice to Articles 12 to 22 of Regulation (EU) 2016/679, the electronic communication services providers</b> shall obtain the consent of <del>end-users who are natural persons</del> <b>users</b> to include their personal data in the <b>publicly available</b> directory and, consequently, shall obtain consent from these <del>end-users</del> <b>users</b> for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory. <b>Electronic communication service providers shall give users the means to verify,</b>	1. The providers of <del>publicly available directories</del> <b>number-based interpersonal communications services</b> shall obtain the consent of end-users who are natural persons to include their personal data in the directory and, <del>consequently, shall obtain consent from these end-users</del> for inclusion of <b>such</b> data per category of personal data, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory. <del>Providers shall give end-users who are natural persons the means to verify, correct and delete such data.</del>	1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>correct, update, supplement and delete such data as determined by the provider of the directory. When electronic communication service providers obtain consent of users, they shall give end-users who are natural persons the means to verify, correct and delete such data make users' data available for public directory providers in an immediate, non-discriminatory and fair manner.</i></p> <p>AM 128</p>		
Article 15(1a)				
155a			<p><b>1a. Notwithstanding paragraph 1, Member States may provide by law that the inclusion of personal data of an end-user who is a natural person in a publicly available directory can take place provided that the end-user who is a natural person shall have the right to object to such inclusion.</b></p>	
Article 15(2)				
156	<p>2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the</p>	<p>2. The providers of a publicly available directory shall inform <del>end-users who are natural persons</del> users whose personal data are in the directory of the available search</p>	<p>2. The providers of a publicly available directory <del>number-based interpersonal communications services</del> shall inform end-users who are natural persons whose personal</p>	<p>3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	directory and obtain end-users' consent before enabling such search functions related to their own data.	functions of the directory and <del>obtain end-users' consent before enabling</del> <b>provide the users the option to disable</b> such search functions related to their own data.  AM 129	data are in the directory of <del>the available search functions of any</del> <b>search function that is not based on name or number in the directory</b> and obtain <del>end-users' the</del> consent of <b>end-users'</b> before enabling such search functions related to their own data.	minimum of other identifiers, additional consent be asked of the subscribers.
Article 15(3)				
157	3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.	3. The <del>providers of publicly available directories</del> <b>electronic communication service providers</b> shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. <b>Electronic communication service</b> providers shall give such end-users that are legal persons the means to verify, correct and delete such data. <b>For the purposes of this Article, natural persons acting in a professional capacity, such as independent professionals, operators of small businesses or freelancers, shall be equated with legal persons, as regards their data related to their professional capacity.</b>  AM 130	3. The providers of <del>publicly available directories</del> <b>number-based interpersonal communications services</b> shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. <del>Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.</del>	4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.
Article 15(3a)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
157a			3a. The providers of number-based interpersonal communications services shall give end-users the means to verify, correct and delete data included in a publicly available directory.	
Article 15(3aa)				
157b			3aa. Notwithstanding paragraphs 1aa to 3a, Member States may provide by law that the requirements under those paragraphs apply to providers of publicly available directories, in addition to or instead of, providers of number-based interpersonal communications services.	
Article 15(4)				
158	4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.	4. <b><i>Without prejudice to Article 12(5) of Regulation (EU) 2016/679, the information to the users and the possibility</i></b> <del>The possibility for end-users</del> not to be included in a publicly available directory, or to verify, correct, <b><i>update, supplement</i></b> and delete any data related to them shall be provided free of charge <b><i>and in an easily accessible manner by the electronic communication services</i></b>	4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.	2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>providers.</i> AM 131		directory, verifying, correcting or withdrawing personal data from it shall be free of charge.
Article 15(4a)				
158a		<i>4a. Where the personal data of the users of number- based interpersonal communications services have been included in a publicly available directory before this Regulation enters into force, the personal data of such users may remain included in a publicly available directory, including versions with search functions, unless the users have expressed their objection against their data being included in the directory or against available search functions related to their data.</i> AM 132	<b>4a. Where the personal data of the end-users of number based interpersonal communications services have been included in a publicly available directory before this Regulation enters into force, the personal data of such end-users may remain included in a publicly available directory, including version with search functions, unless the end-users have expressed their objection against their data being included in the directory or against the use of available search functions related to their data.</b>	
Article 16				
159	Article 16 Unsolicited communications	Article 16 Unsolicited communications	Article 16 Unsolicited <b>and direct marketing</b> communications	Article 13 - Unsolicited communications
Article 16(1)				
160	1. Natural or legal persons may use	1. <b>The use by</b> natural or legal	1. Natural or legal persons <del>may</del>	1. The use of automated calling

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons that have given their consent.	persons <del>may use of electronic communications services, including automated calling, communications systems, semi-automated systems that connect the call person to an individual, faxes, e-mail or other use of</del> electronic communications services for the purposes of <b>presenting or</b> sending direct marketing communications to <del>end-users who are natural persons that</del> users, <b>shall be allowed only in respect of users who</b> have given their <b>prior</b> consent.  AM 133	<del>uses</del> <b>shall be prohibited from using</b> electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons <del>that</del> <b>unless they</b> have given their <b>prior</b> consent.	systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.
Article 16(2)				
161	2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own <b>similar</b> products or services <b>only if</b> customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and	2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own <del>similar</del> products or services <b>only if</b> customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. <b>The customer shall be informed about</b> the right to object	2. <b>Notwithstanding paragraph 1,</b> where a natural or legal person obtains <del>electronic</del> contact details for electronic <del>mail from its customer</del> <b>message from end-users who are natural persons,</b> in the context of the <del>sale</del> <b>purchase</b> of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these <del>electronic</del> contact details for direct marketing of its own <b>similar</b> products or services <b>only if</b> <del>customers</del> <b>such end-users</b> are clearly and distinctly given the opportunity	2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	each time a message is sent.	<i>and</i> shall be given <i>an easy way to exercise it</i> at the time of collection and each time a message is sent. <a href="#">AM 134</a>	to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection <b>of such end-users' contact details and, if that end-user has not initially refused that use, and each time when a natural or legal person sends a message is sent to that end-user for the purpose of direct marketing.</b>	electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.
Article 16(2a)				
161a			<b>2a. Member States may provide by law a set period of time, after the sale of the product or service occurred, within which a natural or legal person may use contact details of the end-user who is a natural person for direct marketing purposes, as provided for in paragraph.</b>	
Article 16(3), introductory part				
162	3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:		<b>3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall: present the calling line identification assigned to them.</b>	3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
				or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.
Article 16(3), point (a)				
163	(a) present the identity of a line on which they can be contacted; or			
Article 16(3), point (b)				
164	(b) present a specific code/or prefix identifying the fact that the call is a marketing call.			
Article 16(3a)				
164a		<i>3a. The masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited communications for direct marketing purposes is prohibited.</i>  AM 135		
Article 16(3a)				
164b			<b>3a. Member States may require natural or legal person using electronic communications</b>	4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			services for the purposes of placing direct marketing calls to present a specific code or prefix identifying the fact that the call is a direct marketing call in addition to the obligation set out in paragraph 3. Member State requiring the use of such a specific code or prefix shall make it available for the natural or legal persons who use electronic communications services for the purposes of direct marketing calls.	concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.
Article 16(4)				
165	4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.	4. Notwithstanding paragraph 1, <del>Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons</del> users shall only be allowed in respect of <del>end-users who are natural persons</del> users who have not expressed their objection to receiving those communications. <del>Member States shall provide that users can object to receiving the direct marketing voice-to-voice calls via a Do Not Call Register, thereby also ensuring that the user needs to opt- out only once.</del>  AM 136	4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.	5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 16(5)				
166	5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected.		5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to <del>unsolicited</del> <b>direct marketing</b> communications sent by means set forth under paragraph 1 are sufficiently protected.	
Article 16(6)				
167	6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications.	6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner <b>and free of charge</b> , to receiving further marketing communications.  AM 137	6. Any natural or legal person using electronic communications services to <del>transmitsend</del> direct marketing communications shall, <b>each time a direct inform end users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications sent:</b>	
Article 16(6), point (a)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
167a			(a) reveal his or its identity and use effective return addresses or numbers;	
Article 16(6), point (b)				
167b			(b) inform end-users of the marketing nature of the communication and the identity and contact details of the legal or natural person on behalf of whom the direct marketing communication is sent;	
Article 16(6), point (c)				
167c			(c) clearly and distinctly give the end-users who are natural persons a means to object or to withdraw their consent, free of charge, at any time, and in an easy and effective manner, to receiving further direct marketing communications, and shall provide the necessary information to this end. This means shall also be given at the time of collection of the contact details according to paragraph 2. It shall be as easy to withdraw as to give consent.	
Article 16(7)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
168	7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.	7. The Commission shall be empowered to adopt implementing measures in accordance with Article <del>26(2)</del> <b>26(1)</b> specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.  AM 138	Deleted	
Article 17				
169	Article 17 Information about detected security risks	Article 17 Information about detected security risks	Deleted	
Article 17(1)				
170	In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.	<del>1. In the case of a particular risk that may compromise</del> <b>Providers of electronic communications services shall comply with the security obligations as prescribed Regulation (EU) 2016/679 and [European Electronic Communications Code]. As regards</b> the security of networks and <del>electronic communications services, the provider of an services and related security obligations, the obligations of Article 40 of the [European Electronic Communications serviceCode] shall inform end-users concerning such</del>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><del>risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved</del>  <b>apply mutatis mutandis to all services in the scope of this Regulation. This Article shall be without prejudice to the obligations provided for in Articles 32 to 34 of Regulation (EU) 2016/679 and the obligations provided for in Directive (EU) 2016/1148.</b></p> <p>AM 139</p>		
Article 17, first paragraph a				
170a		<p><b>1a. Providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the confidentiality and integrity of the communication in transmission or stored are also guaranteed by technical measures according to the state of the art, such as cryptographic methods including end-to-end encryption of the electronic communications data. When encryption of electronic</b></p>		<p>(Article 4) Security  1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.</p>

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>communications data is used, decryption by anybody else than the user shall be prohibited. Notwithstanding Articles 11a and 11b of this Regulation, member States shall not impose any obligations on electronic communications service providers or software manufacturers that would result in the weakening of the confidentiality and integrity of their networks and services or the terminal equipment, including the encryption methods used.</i></p> <p>AM 140</p>		
Article 17, first paragraph b				
170b		<p><i>1b. Providers of electronic communications services, providers of information society services, and manufacturers of software permitting the retrieval and presentation of information on the internet shall not use any means, no matter if technical, operational, or by terms of use or by contracts, that could prevent users and subscribers from applying the best available techniques against intrusions and interceptions and to secure their networks, terminal equipment and electronic</i></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><b>communications. Notwithstanding Articles 11a and 11b of this Regulation, breaking, decrypting, restricting or circumventing such measure taken by users or subscribers shall be prohibited.</b></p> <p>AM 141</p>		
Article 17, first paragraph c				
170c		<p><b><i>1c. In the case of a particular risk that may compromise the security of networks, electronic communications services, information society services or software, the relevant provider or manufacturer shall inform all subscribers of such a risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform subscribers of any possible remedies. It shall also inform the relevant manufacturer and service provider.</i></b></p> <p>AM 142</p>		<p>2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.</p>
CHAPTER IV				
171	CHAPTER IV INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT	CHAPTER IV INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 18				
172	Article 18 Independent supervisory authorities	Article 18 Independent supervisory authorities	Article 18 <del>Independent</del> Supervisory authorities	
Article 18(-1)				
172a			<p><b>-1. Each Member State shall provide for one or more independent public authorities meeting the requirements set out in Articles 51 to 54 of Regulation (EU) 2016/679 to be responsible for monitoring the application of this Regulation.</b></p> <p><b>Member States may entrust the monitoring of the application of Articles 12 to 16 to the supervisory authority or authorities referred to in the previous subparagraph or to another supervisory authority or authorities having the appropriate expertise.</b></p>	
Article 18(1)				
173	1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also	1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also	Deleted	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.	be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. <i>Where Regulation (EU) 2016/679 refers to data subjects, the tasks and powers of the supervisory authorities shall be exercised with regard to end-users under this Regulation. Where Regulation (EU) 2016/679 refers to data controllers, the tasks and powers of the supervisory authorities shall be exercised with regard to providers of electronic communications services and information society services, and manufacturers of software under this Regulation.</i> <a href="#">AM 143</a>		
Article 18(1ab)				
173a			<b>1ab. The supervisory authorities shall have investigative and corrective powers, including the power to impose administrative fines pursuant to Article 23.</b>	
Article 18(1b)				
173b			<b>1b. Where more than one supervisory authority is responsible for monitoring the</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			application of this Regulation in a Member State, such authorities shall cooperate with each other to the extent necessary to perform their tasks.	
Article 18(2)				
174	2. The supervisory authority or authorities referred to in paragraph 1 shall cooperate whenever appropriate with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code].		2. <del>Where the supervisory authority or authorities are not the supervisory authorities referred to in paragraph 1</del> <b>responsible for monitoring the application of Regulation (EU) 2016/679, they</b> shall cooperate <b>with the latter and</b> , whenever appropriate, with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code](EU) <b>2018/1972 and other relevant authorities.</b>	
Article 19				
175	Article 19 European Data Protection Board	Article 19 European Data Protection Board	Article 19 European Data Protection Board	
Article 19, first paragraph, introductory part				
176	The European Data Protection Board, established under Article 68		<b>1</b> The European Data Protection Board, established under Article 68	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	of Regulation (EU) 2016/679, shall have competence to ensure the consistent application of this Regulation. To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679. The Board shall also have the following tasks:		of Regulation (EU) 2016/679, shall have <del>competence to ensure the consistent application of this Regulation. To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679. The Board shall also have the following tasks:</del> <b>the task to contribute to the consistent application of Chapters I II and III of this Regulation.</b>	
Article 19, 2nd paragraph				
176a			<b>2 To that end, the Board shall have the following tasks:</b>	
Article 19, first paragraph, point (a)				
177	(a) advise the Commission on any proposed amendment of this Regulation;		(a) advise the Commission on any proposed amendment of this Regulation;	
Article 19, first paragraph, point (b)				
178	(b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices		(b) examine, on its own initiative, on request of <del>one of its members</del> <b>a supervisory authority designated in accordance with Article 18 (0)</b> or on request of the Commission, any question covering the	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	in order to encourage consistent application of this Regulation.		application of this Regulation <b>in relation to Chapters I, II and III</b> and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation-;	
Article 19, first paragraph, point (ba)				
178a		<i>(ba) draw up guidelines for supervisory authorities concerning the application of Article 9(1) and the particularities of expression of consent by legal entities;</i>  AM 144		
Article 19, first paragraph, point (bb)				
178b		<i>(bb) issue guidelines to determine which technical specifications and signalling methods fulfil the conditions and objectives pursuant to Article 10(1a);</i>  AM 145		
Article 19, first paragraph, point (bc)				
178c		<i>(bc) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph for the</i>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>purpose of further specifying the criteria and requirements for types of services that may be requested for purely individual or work-related usage as referred to in Article 6(3a);</i></p> <p>AM 146</p>		
Article 19, first paragraph, point (bd), introductory part				
178d		<p><i>(bd) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph for the purpose of further specifying the criteria and requirements for:</i></p> <p>AM 147</p>		
Article 19, first paragraph, point (bd)(i)				
178e		<p><i>i measuring the reach of an information society service referred to in Article 8(1) point (d);</i></p> <p>AM 147</p>		
Article 19, first paragraph, point (bd)(ii)				
178f		<p><i>ii security updates referred to in Article 8(1) point (da);</i></p> <p>AM 147</p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 19, first paragraph, point (bd)(iii)				
178g		<i>iii the interference in the context of employment relationships referred to in Article 8(1) point (db);</i> AM 147		
Article 19, first paragraph, point (bd)(iv)				
178h		<i>iv the processing of information emitted by the terminal equipment referred to in Article 8(2);</i> AM 147		
Article 19, first paragraph, point (bd)(v)				
178i		<i>v technical specifications and signalling methods that fulfil the conditions for consent and objection pursuant to Article 8(2a);</i> AM 147		
Article 19, first paragraph, point (bd)(vi)				
178j		<i>vi software settings referred to in Article 10(1a) and (1b); and</i> AM 147		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 19, first paragraph, point (bd)(vii)				
178k		<i>vii technical measures to ensure confidentiality and integrity of the communication pursuant to Article 17(1a), (1b) and (1c)</i> AM 147		
Article 19(d)				
178l			<b>(d) issue guidelines, recommendations and best practices in order to facilitate cooperation, including exchange of information, between supervisory authorities referred to in paragraph x of Article 18 and/or the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679;</b>	
Article 19(da)				
178m			<b>(da) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph to assess for different types of electronic communications services the moment in time of receipt of electronic communications</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			content;	
Article 19(db)				
178n			(db) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph on the provision of consent in the context of Articles 6 to 6b and 8 of this Regulation by end-users who are legal persons or in an employment relationship;	
Article 19(e)				
178o			(e) provide the Commission with an opinion on the icons referred to in paragraph 3 of Article 8;  (f) and (g) deleted	
Article 19(h)				
178p			(h) promote the exchange of knowledge and documentation on legislation on protection of electronic communications of end-users and of the integrity of their terminal equipment as laid down in Chapter II and practice relevant supervisory authorities world wide;	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 19, paragraph 3				
178q			(3) Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.	
Article 19, paragraph 4				
178r			(4) The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and make them public.	
Article 19, paragraph 5				
178s			(5) The Board shall consult the supervisory authorities referred to in Article 18 (0) before any of the tasks referred to in paragraph 2.	
Article 19, paragraph 6				
178t			(6) The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			shall, without prejudice to Article 76 of Regulation (EU) 2016/679, make the result of the consultation procedures publicly available.	
Article 20				
179	Article 20 Cooperation and consistency procedures		Article 20 <del>Cooperation and consistency procedures</del> <b>Cross-border cooperation</b>	
Article 20, first paragraph				
180	Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII of Regulation (EU) 2016/679 regarding the matters covered by this Regulation.		Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. <del>For this purpose, the supervisory authorities shall</del> <b>and</b> cooperate with each other and the Commission in accordance with Chapter VII of Regulation (EU) 2016/679 regarding the matters covered by this Regulation <b>with the Commission.</b>	
CHAPTER V				
181	CHAPTER V REMEDIES, LIABILITY AND PENALTIES	CHAPTER V REMEDIES, LIABILITY AND PENALTIES	CHAPTER V REMEDIES, LIABILITY AND PENALTIES	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 21				
182	Article 21 Remedies	Article 21 Remedies	Article 21 Remedies	
Article 21(1)				
183	1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679.	1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services <b><i>and, where applicable, everybody, organisation or association,</i></b> shall have the same remedies provided for in Articles 77, 78, <del>79 and 80 and 79</del> of Regulation (EU) 2016/679.  AM 148	1. Without prejudice to any other administrative or judicial remedy, every end-user <b>shall have the right to an effective judicial remedy in relation to any infringement of rights under this Regulation, the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy against any legally binding decision of a supervisory authority concerning them</b> of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679.	
Article 21(1a)				
183a		<b><i>1a. Without prejudice to any other administrative or non-judicial remedy, every end-user of electronic communications services shall have the right to an effective judicial remedy against a legally binding decision of a supervisory</i></b>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>authority concerning him or her. End-users shall also have such a right where the supervisory authority does not handle a complaint or does not inform the end- user within three months on the progress or outcome of the complaint lodged. Proceedings against a supervisory authority shall be brought before the court of the Member State where the supervisory authority is established.</i></p> <p>AM 149</p>		
Article 21(1b)				
183b		<p><i>1b. Every end-user of the communications services shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed. Those proceedings against a provider of electronic communication service, the provider of a publicly available directory, software provider enabling electronic communication or persons sending direct marketing commercial communications or collecting information related to or stored in the end-users terminal equipment shall be brought before</i></p>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<p><i>the courts of the Member State where they have an establishment. Alternatively, such proceedings shall be brought before the court of the Member State of the habitual residence of the end-user.</i></p> <p>AM 150</p>		
Article 21(1a)				
183c			<b>1a. Articles 77-80 of Regulation (EU) 2016/679 shall apply mutatis mutandis.</b>	
Article 21(2)				
184	2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation and having a legitimate interest in the cessation or prohibition of alleged infringements, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.		2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation <del>and having a legitimate interest in the cessation or prohibition of alleged infringements</del> , including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.	
Article 22				
185	Article 22 Right to compensation and liability	Article 22 Right to compensation and liability	Article 22 Right to compensation and liability	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 22, first paragraph				
186	Any end-user of electronic communications services who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered, unless the infringer proves that it is not in any way responsible for the event giving rise to the damage in accordance with Article 82 of Regulation (EU) 2016/679.		Any <del>end-user of electronic communications services</del> <b>person</b> who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered, <del>unless the infringer proves that it is not in any way responsible for the event giving rise to the damage</del> in accordance with Article 82 of Regulation (EU) 2016/679.	
Article 23				
187	Article 23 General conditions for imposing administrative fines	Article 23 General conditions for imposing administrative fines	Article 23 General conditions for imposing administrative fines	
Article 23(1)				
188	1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation.	1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation, <b><i>mutatis mutandis</i></b> .  <a href="#">AM 151</a>	1. <del>For the purpose of this Article, Chapter VII</del> <b>83</b> of Regulation (EU) 2016/679 shall apply <b><i>mutatis mutandis</i></b> to infringements of this Regulation.	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 23(2), introductory part				
189	2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:		2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:	
Article 23(2), point (a)				
190	(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;	(a) <del>the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;</del> AM 152 deleted	(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;	
Article 23(2), point (aa)				
190a		(aa) <del>the obligations of the providers of electronic communications services pursuant to Article 11c;</del> AM 153		
Article 23(2), point (b)				
191	(b) the obligations of the provider of	(b) <del>the obligations of the provider of</del>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	software enabling electronic communications, pursuant to Article 10;	<del>software enabling electronic communications, pursuant to Article 10;</del> AM 154 deleted	Deleted	
Article 23(2), point (ba)				
191a		<i>(ba) the obligations of the providers of publicly available number-based interpersonal communication services pursuant to Articles 12, 13 and 14.</i> AM 155		
Article 23(2), point (c)				
192	(c) the obligations of the providers of publicly available directories pursuant to Article 15;		(c) the obligations of the providers of publicly available directories pursuant to Article 15;	
Article 23(2), point (d)				
193	(d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.		(d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.	
Article 23(2), point (e)				
193a			<b>(e) the obligation to designate a</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
			representative pursuant to Article 3 number 2.	
Article 23(3)				
194	3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	3. Infringements of the <del>principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7</del> following provisions of this Regulation shall, in accordance with paragraph 1 <del>of this Article</del> , be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.:  AM 156	3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	
Article 23(3), point (a)				
194a		(a) the principle of confidentiality of communications pursuant to Article 5;  AM 157		
Article 23(3), point (b)				
194b		(b) the permitted processing of		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>electronic communications data, pursuant to Article 6;</i> <a href="#">AM 158</a>		
Article 23(3), point (c)				
194c		<i>(c) the time limits for erasure and the confidentiality obligations pursuant to Article 7;</i> <a href="#">AM 159</a>		
Article 23(3), point (d)				
194d		<i>(d) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;</i> <a href="#">AM 160</a>		
Article 23(3), point (e)				
194e		<i>(e) the requirements for consent pursuant to Article 9;</i> <a href="#">AM 161</a>		
Article 23(3), point (f)				
194f		<i>(f) the obligations of the provider of software enabling electronic</i>		

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
		<i>communications, pursuant to Article 10;</i> AM 162		
Article 23(3), point (g)				
194g		<i>(g) the obligations of the providers of electronic communications services, of the providers of information society services, or of the manufacturers of software permitting the retrieval and presentation of information on the internet pursuant to Article 17.</i> AM 163		
Article 23(4)				
195	4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17.	<del>4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17</del> <i>In the event that the same act or omission by the same person results in non-compliance with both Regulation (EU) 2016/679 and this Regulation, then the maximum administrative fine shall be no more than the maximum administrative fine applicable under this Regulation for that type of infringement.</i> AM 164	4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, <del>14, and 17</del> <b>and 14.</b>	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 23(5)				
196	5. Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.		5. Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	
Article 23(6)				
197	6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.		6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.	
Article 23(7)				
198	7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective		7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	judicial remedy and due process.		judicial remedy and due process.	
Article 23(8)				
199	8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.		8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.	
Article 24				
200	Article 24 Penalties	Article 24 Penalties	Article 24 Penalties	
Article 24(1)				
201				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.		1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.	
Article 24(2)				
202	2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than 18 months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.		2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than <del>18</del> 48 months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.	
CHAPTER VI				
203	CHAPTER VI DELEGATED ACTS AND IMPLEMENTING ACTS	CHAPTER VI DELEGATED ACTS AND IMPLEMENTING ACTS	CHAPTER VI DELEGATED ACTS AND IMPLEMENTING ACTS	
Article 25				
204	Article 25 Exercise of the delegation	Article 25 Exercise of the delegation	Article 25 Exercise of the delegation	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 25(1)				
205	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.		1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	
Article 25(2)				
206	2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation].		2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation].	
Article 25(3)				
207	3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.		3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 25(4)				
208	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016.		4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016.	
Article 25(5)				
209	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.		5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	
Article 25(6)				
210	6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not		6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
	object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.		object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	
Article 26				
211	Article 26 Committee	Article 26 Committee	Article 26 Committee	
Article 26(1)				
212	<p>1. The Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code]. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011<sup>1</sup>.</p> <p>1. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13–18).</p>	<p>1. <b><i>For the purpose of Articles 13(2) and 16(7)</i></b>, the Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code]. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011<sup>1</sup>.</p> <p>1. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13–18).</p> <p>AM 165</p>	<p>1. The Commission shall be assisted by the Communications Committee established under Article 110 of the <del>{118 of Directive establishing the European Electronic Communications Code}</del>(EU) <b>2018/1972</b>. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011<sup>11</sup>.</p> <p><del>1. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13–18).</del></p>	
Article 26(2)				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
213	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.		2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	
CHAPTER VII				
214	CHAPTER VII FINAL PROVISIONS	CHAPTER VII FINAL PROVISIONS	CHAPTER VII FINAL PROVISIONS	
Article 27				
215	Article 27 Repeal	Article 27 Repeal	Article 27 Repeal	
Article 27(1)				
216	1. Directive 2002/58/EC is repealed with effect from 25 May 2018.	1. Directive 2002/58/EC <del>is</del> <b>and Commission Regulation 611/2013 are</b> repealed with effect from <del>25 May 2018</del> <b>[XXX]</b> .  AM 166	1. Directive 2002/58/EC is repealed with effect from <del>25 May 2018</del> <b>[1 August 2022]</b> .	
Article 27(2)				
217	2. References to the repealed Directive shall be construed as references to this Regulation.		2. References to the repealed Directive shall be construed as references to this Regulation.	
Article 28				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
218	Article 28 Monitoring and evaluation clause	Article 28 Monitoring and evaluation clause	Article 28 Monitoring and evaluation clause	
Article 28, first paragraph				
219	By 1 January 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.	By <del>1 January 2018</del> <b>[the date of entry into force of this Regulation]</b> at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.  AM 167	By <b>[1 August 2024]</b> <del>1 January 2018</del> at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.	
Article 28, second paragraph				
220	No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.		No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.	

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
Article 29				
221	Article 29 Entry into force and application	Article 29 Entry into force and application	Article 29 Entry into force and application	
Article 29(1)				
222	1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.		1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	
Article 29(2), first subparagraph				
223	2. It shall apply from 25 May 2018.	2. It shall apply from <del>25 May 2018</del> <i>[one year the date of entry into force of this Regulation]</i> . <a href="#">AM 168</a>	2. <del>¶</del> <b>This Regulation</b> shall apply from <del>25 May 2018</del> <b>[24 months from the date of entry into force of this Regulation]</b> .	
Article 29(2), second subparagraph				
224	This Regulation shall be binding in its entirety and directly applicable in all Member States.		This Regulation shall be binding in its entirety and directly applicable in all Member States.	
Formula				
225	Done at Brussels,		Done at Brussels,	
Formula				

	Commission Proposal	EP Mandate	st6087/21 Council Mandate	Directive 2002/58/EC
226	For the European Parliament		For the European Parliament	
Formula				
227	The President		The President	
Formula				
228	For the Council		For the Council	
Formula				
229	The President		The President	