

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, ePrivacy-Verordnung – ePrivVO)

Inhaltsverzeichnis

Erwägungsgründe (Recitals).....	2	Article 6c [Previous art 6(2a)] Compatible processing of electronic communications metadata.....	79
CHAPTER I GENERAL PROVISIONS.....	61	Article 6d - Processing of electronic communications data for the purpose of preventing child sexual abuse.....	81
Article 1 - Subject matter.....	61	Article 7 - Storage and erasure of electronic communications data.....	81
Article 2 - Material Scope.....	62	Article 8 - Protection of information stored in and related to <i>end-users'</i> terminal equipment.....	82
Article 3 - Territorial scope and representative.....	64	Article 8 - Protection of information <i>transmitted to</i> , stored in and related to <i>processed by and collected from users'</i> terminal equipment.....	82
Article 4 - Definitions.....	66	Article 8 - Protection of end-users' terminal equipment information.....	82
Article 4a - Consent.....	72	Article 9 - Consent.....	89
Chapter 2.....	73	Article 10 - Information and options for privacy settings to be provided.....	90
PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION <i>STORED IN</i> THEIR TERMINAL EQUIPMENT.....	73	Article 11a -Restrictions on the rights of the user.....	93
PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION <i>PROCESSED BY AND RELATED TO</i> THEIR TERMINAL EQUIPMENT.....	73	Article 11b - Restrictions on confidentiality of communications.....	94
Article 5.....	73	Article 11 c - Documentation and reporting of restrictions.....	94
Confidentiality of electronic communications <i>data</i>	73	CHAPTER III - NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS.....	96
Confidentiality of electronic communications.....	73	CHAPTER III <i>END-USERS'</i> RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS...96	
Article 6.....	74	Article 12 - Presentation and restriction of calling and connected line identification.....	97
<i>Permitted</i> processing of electronic communications data.....	74	Article 13 -Exceptions to presentation and restriction of calling and connected line identification.....	98
<i>Lawful</i> processing of electronic communications data.....	74	Article 13 Exceptions to presentation and restriction of calling and connected line identification <i>in relation to emergency communications</i>	98
Article 6a [previous art. 6(3)] Permitted processing of electronic communications content.....	76		
Article 6b [previous art 6(2)] Permitted processing of electronic communications metadata.....	77		

Article 14 - Incoming call blocking.....	100	Article 20 - <i>Cross-border</i> cooperation.....	112
Article 14 Blocking <i>Unwanted, malicious or nuisance calls</i>	100	CHAPTER V - REMEDIES, LIABILITY AND PENALTIES.....	112
Article 15 - Publicly available directories.....	100	Article 21 - Remedies.....	112
Article 16 - Unsolicited communications.....	102	Article 23 - General conditions for imposing administrative fines.....	114
Article 16 - Unsolicited <i>and direct marketing</i> communications.....	102	Article 24 - Penalties.....	117
CHAPTER IV - INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT		CHAPTER VI - DELEGATED ACTS AND IMPLEMENTING ACTS.....	117
.....	108	Article 25 - Exercise of the delegation.....	117
Article 18 - <i>Independent</i> supervisory authorities.....	108	Article 26 - Committee.....	118
Article 18 - Supervisory authorities.....	108	CHAPTER VII - FINAL PROVISIONS.....	118
Article 19 - European Data Protection Board.....	109	Article 27 - Repeal.....	118
Article 20 - Cooperation <i>and consistency procedures</i>	112	Article 28 - Monitoring and evaluation clause.....	118

EU-Kommission ¹	EU-Parlament ²	EU-Rat ³
Erwägungsgründe (Recitals)		
(1) Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be	(1) Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be	(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 private and family life, home and communications. Respect for the confidentiality of one's communications is an essential dimension of this right, applying both to natural and legal persons. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including

1 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52017PC0010>

2 https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html#title2

3 <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>

EU-Kommission	EU-Parlament	EU-Rat
<p>revealed to anyone other than to the parties <i>involved in a communication</i>. 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 <i>personal</i> messaging provided through social media.</p>	<p>revealed to anyone other than to the <i>communicating</i> parties. The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e-mail, internet phone calls and <i>inter-personal</i> messaging provided through social media. <i>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.</i></p>	<p>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.</p>
<p>(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and</p>	<p>(2) The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communications, such as their social relationships, their habits and</p>	<p>- unverändert / not changend -</p>

EU-Kommission	EU-Parlament	EU-Rat
activities of everyday life, their interests, tastes etc.	activities of everyday life, their interests, tastes etc. <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 religion, freedom of assembly, freedom of expression and information.</i>	
		<i>(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 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.</i>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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</p>
<p>(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council 21 , also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this</p>	<p>- unverändert / not changend -</p>	<p>(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value and the protection of which allows legal persons to conduct their business, supporting among other innovation. Therefore, the provisions of this Regulation should in principle apply to both natural and legal persons. Furthermore, this Regulation should ensure that, where necessary, provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council [1], also apply <i>mutatis mutandis</i>⁴ to end-users who are legal persons. This includes the definition of provisions on consent under Regulation (EU) 2016/679.</p>

4 „nachdem die zu ändernden Dinge geändert worden sind “ (vgl. <https://www.dwds.de/wb/mutatis%20mutandis>)

EU-Kommission	EU-Parlament	EU-Rat
Regulation regarding legal persons.		
(4) Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data may include personal data as defined in Regulation (EU) 2016/679.	(4) Pursuant to Article 8(1) of the Charter and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of personal data concerning him or her. Regulation (EU) 2016/679 lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Electronic communications data are generally personal data as defined in Regulation (EU) 2016/679.	- <i>unverändert / not changend</i> -
(5) The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation.	(5) The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. On the contrary, it aims to provide additional and complementary safeguards take into account the need for additional protection as regards the confidentiality of communications. Processing of electronic communications data should only be permitted in accordance with, this Regulation.	- <i>gelöscht / deleted</i> -
(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and	(6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and	- <i>unverändert / not changend</i> -

EU-Kommission	EU-Parlament	EU-Rat
<p>of the Council²² remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of online behaviour of end-users, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.</p>	<p>of the Council²² remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of users. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.</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 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.</p>	<p>(7) The European Data Protection Board should, where necessary, issue guidance and opinions, within the limits of this Regulation, to maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. Cooperation and consistency between Member States, in particular between national Data Protection Authorities, is essential to maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.</p>	<p>- unverändert / not changend -</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>(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 authority.</p>
<p>(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.</p>	<p>(8) This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to software providers permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing commercial communications or collect information transmitted to, stored in, related to or processed by users' terminal equipment.</p>	<p>(8) This Regulation should apply to providers of electronic communications services, and to providers of publicly available directories. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing commercial communications or make use of processing and storage capabilities of terminal equipment or collect information processed by or emitted by or stored in end-users' terminal equipment.</p>
		<p>(8aaa) 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 service provider or person processing such data is established or located in the Union or not.</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>(8aa) 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 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, is should not be covered by this Regulation. For the</p>

EU-Kommission	EU-Parlament	EU-Rat
		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.
		(8a) This Regulation does not apply to the electronic communications data of deceased persons. Member States may provide for rules regarding the processing of electronic communications data of deceased persons.
<p>(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.</p>	<p>(9) This Regulation should apply to electronic communications data processed in connection with the offering and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union. <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></p>	<p>- gelöscht / deleted -</p>

EU-Kommission	EU-Parlament	EU-Rat
<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 23 . 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>(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. <i>In order to ensure</i> an effective and equal protection of end-users when using functionally equivalent services, <i>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]. That definition encompasses</i> 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. <i>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</i></p>	<p>(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services, <i>also known as "over-the-top-services" (OTTs). This Regulation aims at ensuring</i> an effective and equal protection of end-users when using functionally equivalent services, <i>so as to ensure the confidentiality of their communications, irrespective</i> of the <i>technological medium chosen. It does</i> not only <i>cover</i> 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.</p>	<p>(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. In order to ensure an effective and equal protection of end-users when using functionally equivalent services, this Regulation uses the definition of electronic communications services set forth in the Directive (EU) 2018/1972. 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.</p>

EU-Kommission	EU-Parlament	EU-Rat
<i>functionality should be covered by this Regulation.</i>		
		<p>(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.</p>
		<p>(11aa) In all the circumstances 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</p>

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

EU-Kommission	EU-Parlament	EU-Rat
<i>Directive 2014/53/EU.</i>		<p>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, 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, this Regulation should not apply. Typically, providers of machine-to-machine or Internet of Things services operate at the application layer (on top of electronic 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.</p>
<p>(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</p>	<p>(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as wireless internet access points situated at different places within a city, for example department stores, shopping malls, hospitals, airports, hotels and restaurants. Those access points might require a log in or provide a password and might be provided also by</p>	<p>(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, regardless if these networks are secured with</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>through such networks should be protected. <i>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.</i> 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 <i>the corporation.</i></p>	<p><i>public administrations, including Union bodies and agencies.</i> To the extent that those communications networks are provided to <i>users,</i> the confidentiality of the communications transmitted through such networks should be protected. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. <i>This Regulation should also apply to closed social media profiles and groups that the users have restricted or defined as private.</i> 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> <i>The mere requirement of a password should not be considered as providing access to a closed group of end-users if the access to the service as a whole is provided to an undefined group of end-users.</i></p>	<p><i>passwords or not,</i> the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using <i>publicly available</i> electronic communications services and public <i>electronic</i> communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as <i>home (fixed or wireless) networks or</i> corporate networks <i>or networks to which the,</i> access is limited to a pre-defined group of end-users, e.g. to family members or, members of a corporation. <i>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. As soon as electronic communications data is transferred from such a closed group network to a public electronic communications network, this Regulation applies to such data, including when it is M2M/IoT and personal/home assistant data. The provisions of this Regulation regarding the protection of end-users'</i></p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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>
<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 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</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 a user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. It should also include data necessary to identify users' terminal equipment and data emitted by terminal equipment when searching for access points or other equipment. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to</p>	<p>- unverändert / not changend -</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.</p>	<p>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. <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 Regulation which applies to the providers of electronic communications services.</i></p>	
	<p><i>(14 a) Modern electronic communications services, including the Internet and the OTT services that run on top of it, function on the basis of a protocol stack. Each protocol defines content (also called payload), a header and sometimes a trailer. Any higher protocol in the stack would be encapsulated in the content part of a lower level protocol. For example, A TCP segment would be in the content part of an IP packet, whose header would include the source and destination IP addresses between which the IP packet should be routed. TCP segments could contain an SMTP message in their content part, i.e. an e-mail. At the SMTP protocol level, the header would notably contain the sender and receiver email addresses</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>and the content part would contain the message itself. In practice, the header and the trailer of a protocol message correspond to metadata for the given protocol. This means that the metadata on one protocol layer will be content for the lower layers encapsulating the information. Where this Regulation lays down different rules for the processing of content and metadata, this should be understood specifically for the considered electronic communications service and the protocol layer it is operating on. For an Internet service provider, for example, the subject, the sender, the recipient and the body of an email will be altogether considered as content of the IP packets routed by it. However regarding an e-mail provider, only the subject and the body of the email will be considered as content, whereas the recipient and the sender will be considered as metadata. This separation of protocol layers is crucial for maintaining the neutrality of the electronic communications services (net neutrality), which is protected under Regulation (EU) 2015/2120.</i></p>	
<p>(15) Electronic communications data should be treated as confidential. This means that any interference with the transmission of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. The prohibition of interception of</p>	<p>(15) Electronic communications should be treated as confidential. This means that any interference with the transmission of electronic communications, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of all the communicating parties should be prohibited. When the processing is allowed</p>	<p>- unverändert / not changend -</p>

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

EU-Kommission	EU-Parlament	EU-Rat
	<p>Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, and analysis of users' traffic data, including browsing habits without the users' consent.</p>	
		<p>(15aa) 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.</p>
		<p>(15aaa) Moreover, trade secrets are protected in accordance with Directive (EU) 2016/943.</p>
		<p>(15a) 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 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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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 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.</p>
<p>(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 <i>in the</i> electronic communications network. It should not prohibit either the processing of</p>	<p>(16) The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission. It should not prohibit the processing of electronic communications data by public authorities,</p>	<p>(16) The prohibition of processing, including storage of communications is not intended to prohibit any automatic, intermediate and transient processing, including storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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.</p>	<p>computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), providers of electronic communications networks and services and by providers of security technologies and services, in compliance with Regulation 2016/679 and to the extent strictly necessary and proportionate for the sole purposes of ensuring network and information security, [i.e. preservation of availability, integrity], and confidentiality of information, and ensuring the security of the related services offered by, or accessible via, those networks and systems. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communications systems, security services, checking security threats such as the presence of malware, spam or to check against DDoS attacks, or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc. Such processing could be carried out by another party which acts as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service.</p>	<p>network. Processing of electronic communications data by providers of electronic communications services and networks should only be permitted in accordance with this Regulation. It should not prohibit the processing of electronic communications data without consent of the end-user to ensure the security, including the availability, authenticity, integrity or confidentiality, of the electronic communications services, including for example checking security threats such as the presence of malware or viruses, or 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>(16a) The protection of the content of electronic communications pertains to the essence of the</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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 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 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</p>

EU-Kommission	EU-Parlament	EU-Rat
		proportionate for such service.
		<p>(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 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.</p>
		<p>(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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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.</p>
<p>(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. <i>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.</i> However, <i>end-users</i> 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 <i>end-users'</i> 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. <i>Examples of commercial usages of electronic communications metadata by providers of electronic communications services may</i></p>	<p>(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. However, <i>users</i> attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. This Regulation should require providers of electronic communications services to obtain <i>users'</i> consent to process electronic communications metadata, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata. Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and 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</p>	<p>(17) The processing of electronic communications metadata can be useful for businesses, consumers and society as a whole. <i>Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and they also want to control the use of electronic communications metadata for purposes other than conveying the communication. Therefore, providers of electronic communications networks and services should be permitted to process electronic communications metadata after having obtained the end-users' consent. In addition, those providers should be permitted to 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.</i> Examples of commercial usages of electronic communications metadata by providers of electronic</p>

EU-Kommission	EU-Parlament	EU-Rat
<p><i>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.</i></p> <p>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.</p>	<p>the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.</p>	<p>communications services may include the provision of heat maps; a graphical representation of data using colours to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.</p>
	<p><i>(17 a) Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using</i></p>	<p><i>(17aa) Further processing for purposes other than for which the metadata where initially collected may take place without the consent of the end-users concerned, provided that such processing is</i></p>

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>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.</i></p>	<p>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 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>(17a) 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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>emergencies, in particular natural and man-made disasters. Processing of electronic communications metadata of an 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>(17b) 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 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</p>

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

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>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></p>	<p>detriment.</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 <i>interference with the</i> 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 <i>end-users</i> concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. <i>Such consultation should be in</i></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 <i>processing of</i> content <i>data</i> 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 <i>users</i> concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always <i>carry out an impact assessment as provided for in Regulation (EU) 2016/679 and if</i></p>	<p>(19) Third parties are legal or natural person that do not provide an electronic communications service to the end-user concerned. However, sometimes the same legal or natural person can also provide different kind of services to the same end-user, for example 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 communication service, such as automatic storage of the messages in the cloud by web-based email, the provider of such a service normally is not deemed to be a third party.</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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>necessary under that Regulation, consult the supervisory authority prior to the processing. After electronic communications content has been sent by the user and received by the intended user or users, it may be recorded or stored by the user, users or by a third party entrusted by them to record or store such data, which could be the electronic communications service provider. Any processing of such stored communications data where the data is stored on behalf of the user must comply with this Regulation. The user may further process the data and if it contains personal data, must comply with Regulation (EU) 2016/679.</p>	
	<p>(19 a) It should be possible to process electronic communications data for the purposes of providing services explicitly requested by a user for personal or personal work-related purposes such as search or keyword indexing functionality, virtual assistants, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools by persons with disabilities. This should be possible without the consent of all users but may take place with the consent of the user requesting the service. Such consent also precludes the provider from processing those data for other purposes.</p>	
	<p>(19 b) Interference with the confidentiality of metadata</p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>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>(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection.</p>	<p>(20) Terminal equipment of users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes very sensitive data that may reveal details of the behaviour, psychological features, emotional condition and political and social preferences of an individual, including the content of communications, pictures, the location of individuals by accessing the GPS capabilities of the device, contact lists, and other information already stored in the device, the</p>	<p>(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, in particular where such information is processed by, stored in, or collected from such equipment, or where information is collected from it or processed in order to enable it to connect to another device and or network equipment, are part of the end-user's private sphere, including the privacy of one's communications, and require protection in accordance with the Charter of Fundamental Rights of the European Union. 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</p>

EU-Kommission	EU-Parlament	EU-Rat
<p><i>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.</i> Information related to the <i>end-user's</i> 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 <i>end-users</i>. Techniques that surreptitiously monitor the actions of <i>end-users</i>, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the <i>end-users'</i> terminal equipment pose a serious threat to the privacy of <i>end-users</i>. Therefore, any such interference with the <i>end-user's</i> terminal equipment should be allowed only with the <i>end-user's</i> consent and for specific and transparent purposes.</p>	<p>information related to such equipment requires enhanced privacy protection. Information related to the user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these <i>users</i>. <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 <i>users</i>, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the <i>users'</i> terminal equipment pose a serious threat to the privacy of <i>users</i>. Therefore, any such interference with the <i>user's</i> terminal equipment should be allowed only with the <i>user's</i> 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>enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, the <i>use of processing and storage capabilities and the collection of information from</i> end-user's terminal equipment should be allowed only with the end-user's consent and <i>or</i> for <i>other</i> specific and transparent purposes <i>as laid down in this Regulation. The information collected from end-user's terminal equipment can often contain personal data.</i></p>
		<p>(20aa) In light of the principle of purpose limitation laid down in Article 5 (1) (b) of Regulation (EU)</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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>(20aaa) 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 for the subsequent readings of the cookie in the context of a revisit to the same website domain initially visited by the end-user.</p>
		<p>(20aaaa) 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-</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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, 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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>the end-user who requests the service from the provider of the service.</p>
		<p>(20a) 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 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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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>(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website. Information society providers that engage in</p>	<p>(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorising the technical storage or access which is strictly necessary and proportionate for the legitimate purpose of enabling the use of a specific service explicitly requested by the user. This may include the storing of information (such as cookies and other identifiers) for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. Such techniques, if implemented with appropriate privacy safeguards, can also be a legitimate and useful</p>	<p>(21) Use of the processing and storage capabilities of terminal equipment or access to information stored in terminal equipment without the consent of the end-user 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 necessary and proportionate for the purpose of providing a specific service 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, authentication session cookies 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</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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>tool, for example, in measuring web traffic to a website. Such measuring implies that the result of processing is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person. Information society providers could engage in configuration checking in order to provide the service in compliance with the user's settings and the mere logging revealing the fact that the user's device is unable to receive content requested by the user, should not constitute illegitimate access to such a device, or use of the device processing capabilities for which consent is required.</p>	<p>basket. In the area of IoT services 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 of the end-users' energy consumption. The same applies for instance to storing, processing or accessing of information from automated and connected vehicles for security related software updates.</p>
		<p>(21aa) In some cases the use of processing and storage capacities 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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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>(21a) 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 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.</p> <p>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>(21b) Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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 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>(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and</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, users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, users are overloaded with requests to provide consent. <i>This Regulation should prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.</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</p>	<p>- gelöscht / deleted -</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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.</p>	<p>consent by technical specifications, for instance by using the appropriate settings of a browser or other application. Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties. The choices made by users when establishing the general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers, or applications or operating systems may be used as the executor of a user's choices, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.</p>	
<p>(23) The principles of data protection by design and by default were codified under Article 25 of Regulation</p>	<p>(23) The principles of data protection by design and by default are codified under Article 25 of Regulation (EU)</p>	<p>- gelöscht / deleted -</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>(EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in a an easily visible and intelligible manner.</p>	<p>2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software permitting electronic communications (such as browsers, operating systems and communication apps), irrespective of whether the software is obtained separately or bundled with hardware, shall configure the software so that privacy is protected, the cross- domain tracking and the storing of information on the terminal equipment by third parties is prohibited by default. In addition, providers of such software are required to offer sufficiently granular options to consent to each distinct category of purposes. These distinct categories include, at least, the following categories: (i) tracking for commercial purposes or for direct marketing for non-commercial purposes (behavioural advertising); (ii) tracking for personalised content; (iii) tracking for analytical purposes; (iv) tracking of location data; (v) providing personal data to third parties (including providing unique identifiers to match with personal data held by third parties) No consent is required for information that is collected from end-users' terminal equipment when it is strictly necessary for providing an information society service requested by the end-user, for example in order to adapt the screen size to the device, or to remember items in a shopping basket. Web browsers, operating systems and communication apps should allow the end-user to</p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>consent to cookies or other information that is stored on, or read from terminal equipment (including the browser on that equipment) by a specific website or originator even when the general settings prevent the interference and vice versa. With regard to a specific party, web browsers and communication apps should also allow users to separately consent to internet-wide tracking. Privacy settings should also include options to allow the user to decide for example, whether multimedia players, interactive programming language viewers, or similar software can be executed, if a website can collect geo-location data from the user, or if it can access specific hardware such as a webcam or microphone. Such privacy settings should be presented in an easily visible and intelligible manner, and at the moment of installation or first use, users should be informed about the possibility to change the default privacy settings among the various options. Information provided should not dissuade users from selecting higher privacy settings and should include relevant information about the risks associated to allowing cross-domain trackers, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising or sharing with more third parties. Software manufacturers should be required to provide easy ways for users to change the privacy settings at any time during use and to allow the user to make</i></p>	

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

EU-Kommission	EU-Parlament	EU-Rat
<p><i>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.</i></p>		
<p>(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example,</p>	<p>(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to users, for example when they enter stores, with personalised offers. While some of these functionalities do not entail high privacy risks, others do, for example,</p>	<p>(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, the WiFi signal etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer physical movements' tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, such as providing data on the number of people waiting in line, ascertaining the number of people in a specific area, 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</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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>those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should either obtain the user's consent or anonymise the data immediately while limiting the purpose to mere statistical counting within a limited time and space and offering effective opt-out possibilities.</p>	<p>also apply appropriate technical and organisations measures to ensure the level of security appropriate to the risks, including pseudonymisation of the data and making it anonymous or erase it as soon it is no longer needed for this purpose. 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. 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.</p>
		<p>(25a) Processing the information emitted by the terminal equipment to enable it to connect to another device would be permitted if the end-user has given consent or if it is necessary for the provision of a</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>service requested by the end-user. This kind of processing might be necessary for example for the provision of some IoT related services.</p>
<p>(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of</p>	<p>(26) When the processing of electronic communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights.</p>	<p>(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, including by way of derogations, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including public security and the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic communications, including by requiring providers to enable and assist competent authorities in carrying out lawful interceptions, or take other</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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. <i>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).</i></p>		<p>measures, such as legislative measures providing for the retention of data for a limited period of time, 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><i>(26 a) In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design. Member States should not impose any obligation on encryption providers, on providers of electronic communications services or on any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of “backdoors”.</i></p>	
<p>(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</p>		

EU-Kommission	EU-Parlament	EU-Rat
<p>call is being made and the right of the called party to reject calls from unidentified lines. Certain end-users, in particular help lines, and similar organisations, have an interest in guaranteeing the anonymity of their callers. As regards connected line identification, it is necessary to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected.</p>		
<p>(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.</p>	<p>- <i>unverändert / not changend</i> -</p>	<p>(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 malicious or 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. 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 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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>requiring that specific categories or classes of radio equipment support certain features ensuring access to emergency services.</p>
<p>(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.</p>	<p>- <i>unverändert / not changend</i> -</p>	<p>(29) Technology exists that enables providers of electronic communications services to limit the reception of unwanted, malicious or nuisance calls by end-users in different ways, including blocking silent calls and other unwanted, malicious and nuisance calls, 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 number-based interpersonal communications services should deploy this technology and protect end-users against such calls 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.</p>
<p>(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</p>	<p>(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</p>	<p>(30) Publicly available directories means any directory or service containing information on end-users of number-based interpersonal communication services such as name, phone numbers (including mobile phone numbers), email address, home address and includes inquiry services, the main function of which is to enable to identify such end-users. End-users that are</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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.</p>	<p>of the personal data of a natural person requires that users are asked for consent before their personal data are included in a directory. The legitimate interest of legal entities requires that end-users that are legal entities have the right to object to the data related to them being included in a directory. The consent should be collected by the electronic communications service provider at the moment of signing the contract for such service. Natural persons acting in a professional capacity, such as independent professionals, operators of small businesses or freelancers, shall be equated with legal persons, as regards their data related to their professional capacity.</p>	<p>natural persons should be asked for consent before their personal data are included in a directory, unless Member States provide that such end-users have the right to object to inclusion of their personal data. The legitimate interest of legal persons requires that end-users that are legal persons have the right to object to the data related to them being included in a directory. 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.</p>
<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 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</p>	<p>(31) If users give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, electronic communications service providers should inform the users of the purposes of the directory and of the search functions of the directory before including them in that directory. Users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the user's contact details can</p>	<p>(31) Providers of number-based interpersonal communications services should inform the end-users who are natural persons of the search functions of the directory and obtain their consent before enabling such search functions related to their personal data. 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.</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>basis of which the end-user's contact details can be searched should not necessarily be the same.</p>	<p>be searched should not necessarily be the same. The providers or publicly available directories shall provide information about the search functions, as well as if new options and functions of the directories are available in the publicly available directories and provide the users the option to disable such functions.</p>	
<p>(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.</p>	<p>(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services, regardless of the form it takes. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.</p>	<p>(32) In this Regulation, direct marketing communications refers to any form of advertising sent by a natural or legal person directly to one or more specific end-users using publicly available electronic communications services. The provisions on direct marketing communications do should not apply to other form of marketing or advertising that is not sent directly to 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. In addition to direct communications advertising for the offering of products and services for commercial purposes, Member States may decide that direct marketing communications may include direct marketing communications sent by political parties that contact natural persons via publicly available electronic communications services in order to promote their parties. The same applies to messages sent by other non-profit organisations to support the purposes of the</p>

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

EU-Kommission	EU-Parlament	EU-Rat
<p>should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.</p>	<p>possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.</p>	<p>contact details for electronic message in accordance with Regulation (EU) 2016/679.</p>
		<p>(33a) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish and or maintain national systems which allow all or 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.</p>
<p>(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 should indicate the identity of the legal or the natural person transmitting the communication or on behalf of whom</p>	<p>- unverändert / not changend -</p>	<p>(34) When end-users who are natural persons have provided their consent to receiving direct marketing communications, they should still be able to withdraw their consent at any time in an easy manner and without any cost to them. To facilitate effective enforcement of Union rules on direct marketing communications, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending direct marketing communications. Direct marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person sending or the communication and, where applicable, on whose</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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.</p>		<p>behalf the communication is sent and provide the necessary information for end-users who are natural persons to exercise their right to withdraw their consent to receiving further 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.</p>
<p>(35) In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address, which can be easily used by end-users to withdraw their consent. Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should display their identity line on which the company can be called or present a specific code identifying the fact that the call is a marketing call.</p>	<p>- <i>unverändert / not changend</i> -</p>	<p>(35) Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should present their identity line on which the company can be called. 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. Using a specific code or prefix should not relieve the legal or natural persons sending direct marketing call from the obligation to present their calling line identification.</p>
<p>(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on</p>	<p>(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communications systems, given that they are more costly for the sender and impose no financial costs on</p>	<p>- <i>vergessen? - forgotten? -</i></p>

EU-Kommission	EU-Parlament	EU-Rat
<p>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.</p>	<p>end-users, justify the obligation for Member States to establish and or maintain national systems only allowing such calls to end-users who have not objected.</p>	
<p>(37) Service providers who offer electronic communications services should inform end- users of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679.</p>	<p>(37) Service providers who offer electronic communications services should process electronic communications data in such a way as to prevent unauthorised processing, including access, or alteration. They should ensure that such unauthorised access or alteration can be detected, and also ensure that electronic communications data are protected by using state-of the art software and cryptographic methods including encryption technologies. Service providers should also inform users of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679. The obligations of Article 40 of the [European Electronic Communications Code] should apply to all</p>	<p>- gelöscht / deleted -</p>

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>services within the scope of this Regulation as regards the security of networks and services and related security obligations thereto.</i></p>	
<p>(38) To ensure full consistency with Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.</p>	<p>(38) To ensure full consistency with Regulation (EU) 2016/679, The enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. <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</p>	<p>(38) Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The designation of supervisory authorities responsible for the monitoring of the application of this Regulation cannot affect the right of natural persons to have 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 persons should have the same rights as end-users who are natural persons regarding any supervisory authority entrusted to monitor any provisions of 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 additional tasks designated under this Regulation.</p>

EU-Kommission	EU-Parlament	EU-Rat
	financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.	
	<p><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 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>(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</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, <i>including adopting binding decisions</i>, 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</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. 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>

EU-Kommission	EU-Parlament	EU-Rat
<p>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>and effective powers in each Member State, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, without prejudice to the powers of prosecutorial authorities under Member 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>(40) In order to strengthen the enforcement of the rules of this Regulation, each supervisory authority should have the power to impose penalties including administrative fines for any infringement of this Regulation, in addition to, or instead of any other appropriate measures pursuant to this Regulation. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. For the purpose of setting a fine under this Regulation, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 of the Treaty.</p>		
<p>(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</p>	<p>(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons in the provision and use of electronic communications services and in particular their right to respect of their private life and communications with regard to the processing of personal data and to ensure the free movement of personal data within the Union, the power to adopt</p>	<p>- unverändert / not changend -</p>

EU-Kommission	EU-Parlament	EU-Rat
<p>acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016²⁵ . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. 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>acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the user of the terminal equipment can take to minimise the collection. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016²⁵ . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. For instance, implementing measures are necessary to specify a code to identify direct marketing</p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p>calls including those made through automated calling and communications systems. They are also necessary to establish the procedures and circumstances to override the elimination of the presentation of the calling line identification on a temporary basis where users request the tracing of malicious or nuisance calls Those powers should be exercised in accordance with Regulation (EU) No 182/2011.</p>	
<p>(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 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.</p>		
<p>(43) Directive 2002/58/EC should be repealed.</p>		
<p style="text-align: center;">CHAPTER I GENERAL PROVISIONS Article 1 - Subject matter</p>		
<p>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.</p>	<p style="text-align: center;">- <i>unverändert / not changend</i> -</p>	<p>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.</p>
		<p>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</p>

EU-Kommission	EU-Parlament	EU-Rat
		electronic communications services, and in particular their rights to respect of communications.
2.This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, which shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data	- <i>unverändert / not changend</i> -	The free movement of electronic communications data and electronic communications services within the Union shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural persons and the protection of natural persons with regard to the processing of personal data, and for protection of communications of legal persons.
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.	- <i>unverändert / not changend</i> -	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 to 2.
Article 2 - Material Scope		
1. This Regulation applies to	1. This Regulation applies to:	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.	(a) the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services, <i>irrespective of whether a payment is required;</i> (b) the processing of information related to <i>or processed by</i> the terminal equipment of end-users; (c) the placing on the market of software permitting electronic communications including the retrieval and presentation of information on the Internet	(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) end-users' terminal equipment information. (c) the offering of a publicly available directory of end-users of electronic communications services; (d) the sending of direct marketing communications to end-users.

EU-Kommission	EU-Parlament	EU-Rat
	<p>(d) the provision of publicly available directories of users of electronic communications;</p> <p>(e) the sending of direct marketing electronic communications to end-users.</p>	
2. This Regulation does not apply to:		
<p>(a) activities which fall outside the scope of Union law;</p> <p>(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;</p> <p>(c) electronic communications services which are not publicly available;</p> <p>(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;</p>	<p>- unverändert / not changend -</p>	<p>(a) 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 activities whether it is a public authority or a private operator acting at the request of a public authority;</p> <p>(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;</p> <p>(c) electronic communications services which are not publicly available;</p> <p>(d) activities, including data processing 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;</p> <p>(e) electronic communications data processed after receipt by the end-user concerned,</p>
<p>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].</p>		<p>- vergessen? - forgotten? -</p>

EU-Kommission	EU-Parlament	EU-Rat
4.This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.		
5.This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.		
Article 3 - Territorial scope and representative		
1.This Regulation applies to:		
(a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;	(a) the offering of electronic communications services, software, publicly available directories, or direct marketing electronic communications to end-users in the Union, irrespective of whether a payment of the end-user is required;	(a) the provision of electronic communications services to end-users who are in the Union,
		(aa) the processing of electronic communications content and of electronic communications metadata of end-users who are in the Union;
(b) the use of such services;	(b) the activities referred to in Article 2 that are provided from the territory of the Union;	- gelöscht / deleted -
(c) the protection of information related to the terminal equipment of end-users located in the Union.	(c) the processing of information related to or processed by the terminal equipment of end-users that is in the Union.	(c) the protection of terminal equipment information of end-users who are in the Union.
		(cb) the offering of publicly available directories of end-users of electronic communications services who are in the Union; (cc) the sending of direct marketing communications to end-users who are in the Union.
2. Where the provider of an electronic communications	2. Where the provider of an electronic communications	2. Where the provider of an electronic communications

EU-Kommission	EU-Parlament	EU-Rat
<p>service is not established in the Union it shall designate in writing a representative in the Union.</p>	<p>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.</p>	<p>service, 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 is not established in the Union it shall designate in writing, within one month from the start of its activities, a representative in the Union and communicate it to the competent Supervisory Authority.</p>
		<p>2a. The requirements laid down in paragraph 2 shall not apply if 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.</p>
<p>3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.</p>	<p>- unverändert / not changend -</p>	<p>3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.</p>
<p>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 <i>processing electronic communications data</i> for the purposes of ensuring compliance with this Regulation.</p>	<p>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, <i>courts</i>, and end-users, on all issues related to <i>the activities referred to in Article 2</i> for the purposes of ensuring compliance with this Regulation.</p>	<p>4. The representative shall be mandated by the provider or person it represents to be addressed 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.</p>

EU-Kommission	EU-Parlament	EU-Rat
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 <i>processes electronic communications data in connection with the provision of electronic communications services</i> from outside the Union <i>to end-users in the Union.</i>	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 <i>undertakes the activities referred to in Article 2</i> from outside the Union.	5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against the provider or person it represents.
		6. 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.
Article 4 - Definitions		
1. For the purposes of this Regulation, following definitions shall apply: (a) the definitions in Regulation (EU) 2016/679;		
(b) the <i>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</i> of Article 2 of [Directive establishing the European Electronic Communications Code];	(b) the <i>definition of 'call' in point (21)</i> 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 paragraphs (1), (4), (5), (6), (7), (14) and (31) respectively of Article 2 of Directive (EU) 2018/1972 ;
(c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC	- <i>unverändert / not changend</i> -	(c) the definition of 'terminal equipment' in Article 1 (1) of Commission Directive 2008/63/EC;
		(d) the definition of 'information society service' in

EU-Kommission	EU-Parlament	EU-Rat
		point (b) of Article 1 (1) of Directive (EU) 2015/1535.
<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>- gelöscht / deleted -</i></p>	<p>2. For the purposes of this Regulation, the definition of 'interpersonal communications service' referred to in point (b) of paragraph 1 shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.</p>
		<p>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.</p>
<p>3. In addition, for the purposes of this Regulation the following definitions shall apply: (a) 'electronic communications data' means electronic communications content and electronic communications metadata;</p>		
	<p><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 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,</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>irrespective of the type of information conveyed;</i></p> <p><i>(-aa) 'electronic communications service' means a service provided via electronic communications networks, whether for remuneration or not, which encompasses one or more of the following: an 'internet access service' as defined in Article 2(2) or Regulation (EU) 2015/2120; an interpersonal communications service; a service consisting wholly or mainly in the conveyance of the signals, such as a transmission service used for the provision of a machine-to-machine service and for broadcasting, but excludes information conveyed as part of a broadcasting service to the public over an electronic communications network or service except to the extent that the information can be related to the identifiable end-user receiving the information; it also includes services which are not publicly available, but provide access to a publicly available electronic communications network;</i></p> <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><i>(-ac) 'number-based interpersonal communications service' means an interpersonal communications service which connects to the public switched telephone</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>network, either by means of assigned numbering resources, i.e. number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;</i></p> <p><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></p> <p><i>(-ae) 'end-user' means a legal entity or a natural person using or requesting a publicly available electronic communications service;</i></p> <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>(b) 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;</p>	<p>(b) 'electronic communications content' means the content transmitted, distributed or exchanged by means of electronic communications services, such as text, voice, videos, images, and sound. Where metadata of other electronic communications services or protocols are transmitted, distributed or exchanged by using the</p>	<p>- unverändert / not changend -</p>

EU-Kommission	EU-Parlament	EU-Rat
	<i>respective service, they shall be considered electronic communications content for the respective service;</i>	
(c) 'electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;	(c) 'electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content ; including data used to trace and identify the source and destination of a communication, data on the location of the terminal equipment processed in the context of providing electronic communications services, and the date, time, duration and the type of communication;	(c) 'electronic communications metadata' means data processed by means of electronic communications services 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;
(d)'publicly available directory' means a directory of end-users of electronic communications 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;	- unverändert / not changend -	(d) 'publicly available directory' means a directory of end-users of number-based interpersonal communications 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 and the main function of which is to enable identification of such end-users;
(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;	- unverändert / not changend -	(e) 'electronic message ' means any 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, including e-mail, SMS, MMS and functionally equivalent applications and techniques;

EU-Kommission	EU-Parlament	EU-Rat
<p>(f) 'direct marketing communications' means any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.;</p>	<p>(f) 'direct marketing communications' means any form of advertising, whether in written, oral or video format, sent, served or presented to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, fax machines etc.;</p>	<p>(f) 'direct marketing communications' means any form of advertising, whether written or oral, sent via a publicly available electronic communications service directly to one or more specific end-users, including the placing of voice-to-voice calls, the use of automated calling and communication systems with or without human interaction, electronic message etc.;</p>
<p>(g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems;</p>	<p>(g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems, including calls made using automated calling and communications systems which connect the called person to an individual;</p>	<p>- unverändert / not changend -</p>
<p>(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 communication systems which connect the called person to an individual.</p>	<p>(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.</p>	<p>- unverändert / not changend -</p>
		<p>(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.</p>
		<p>(j) 'location data' means data processed by means of an electronic communications network or service,</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;</p>
		<p style="text-align: center;">Article 4a - Consent</p> <p>1. The provisions for consent provided for under Regulation (EU) 2016/679/EU shall apply to natural persons and, <i>mutatis mutandis</i>, to legal persons.</p> <p>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.</p> <p>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 placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.</p> <p>2aa. 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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>equipment is permitted.</p> <p>2a. 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>3. End-users who have consented to the processing of electronic communications data in accordance with this Regulation shall be reminded of the possibility to withdraw their consent at periodic intervals of [no longer than 12 months], as long as the processing continues, unless the end-user requests not to receive such reminders.</p>
Chapter 2		
PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT	PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION PROCESSED BY AND RELATED TO THEIR TERMINAL EQUIPMENT	PROTECTION OF ELECTRONIC COMMUNICATIONS OF END-USERS AND OF THE INTEGRITY OF THEIR TERMINAL EQUIPMENT
Article 5		
Confidentiality of electronic communications data	Confidentiality of electronic communications	<i>- unverändert / not changend -</i>
Electronic communications data shall be confidential. Any interference with electronic communications data , such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or	1. Electronic communications shall be confidential. Any interference, with electronic communications , such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or any	Electronic communications data shall be confidential. Any interference with electronic communications data, including listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance

EU-Kommission	EU-Parlament	EU-Rat
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, by persons other than the end-users , shall be prohibited.	and processing of electronic communications data, by anyone other than the end-users concerned , shall be prohibited, except when permitted by this Regulation.
	1 a. Confidentiality of electronic communications shall also apply to data related to or processed by terminal equipment.	
Article 6		
Permitted processing of electronic communications data	Lawful processing of electronic communications data	<i>- unverändert / not changend -</i>
<p>1. Providers of electronic communications networks and services may process electronic communications data if:</p> <p>(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or</p> <p>(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.</p>	<p>1. Providers of electronic communications networks and services may process electronic communications data only if it is technically necessary to achieve the transmission of the communication, for the duration necessary for that purpose.</p>	<p>1. Providers of electronic communications networks and services shall be permitted to process electronic communications data only if:</p> <p>(a) it is necessary to provide an electronic communication service; or</p> <p>(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults, errors, security risks or attacks on electronic communications networks and services;</p>
	1 b. Providers of electronic communications networks and services or other parties acting on behalf of the provider or the end-user may process electronic communications data only if it is technically necessary to maintain or restore the availability, integrity,	(c) it is necessary to detect or prevent security risks or attacks on end-users' terminal equipment; (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

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>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></p>	<p>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.</p>
<p>2. Providers of electronic communications services may process electronic communications metadata if:</p> <p>(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/212028 for the duration necessary for that purpose; or</p> <p>(b) it is necessary for billing, <i>calculating</i> interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or</p> <p>(c) the <i>end</i>-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 <i>end-users</i>, provided that the purpose or purposes concerned could not be fulfilled <i>by processing information that is made anonymous.</i></p>	<p>2. Providers of electronic communications services <i>and networks</i> may process electronic communications metadata <i>only</i> if:</p> <p>(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) 2015/212028 for the duration <i>technically</i> necessary for that purpose; or</p> <p>(b) it is <i>strictly</i> necessary for billing, <i>determining</i> interconnection payments, detecting or stopping fraudulent <i>use of, or subscription to,</i> electronic communications services; or</p> <p>(c) the user concerned <i>has</i> given <i>his or her</i> consent to the processing of <i>his or her</i> communications metadata for one or more specified purposes, including for the provision of specific services to such <i>users</i>, provided that the purpose or purposes concerned could not be fulfilled <i>without the processing of such metadata.</i></p>	<p>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 processing information that is made anonymous.</p> <p>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.</p>
	<p><i>(2a) For the purposes of point (c) of paragraph 2, where</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>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.</i></p>	
<p>3.Providers of the electronic communications services may process electronic communications content only:</p>	<p>- unverändert / not changend -</p>	<p>Article 6a [previous art. 6(3)] Permitted processing of electronic communications content</p> <p>1. Without prejudice to Article (6) 1, providers of the electronic communications networks and services shall be permitted to process electronic communications content only:</p>
<p>(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</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 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</p>	<p>(a) for the sole purpose of the provision of a specific service requested by the user, if the user concerned has given his or her consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content by the provider; or</p> <p>(b) if all users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the</p>	<p>(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</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.</p> <p>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</p>

EU-Kommission	EU-Parlament	EU-Rat
consultation of the supervisory authority.	consultation of the supervisory authority.	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.
	<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><i>Article 6b [previous art 6(2)] Permitted processing of electronic communications metadata</i></p> <p>1. Without prejudice to Article (6) 1, providers of electronic communications networks and services shall be permitted to process electronic communications metadata only if:</p> <p>(a) it is necessary for the purposes of network management or network optimisation, or to meet technical quality of service requirements pursuant to Directive (EU) 2018/1972 or Regulation (EU) 2015/212020; or</p> <p>(b) it is necessary for the performance of an electronic communications service contract to which the end-user is party, or if necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or</p> <p>(c) the end-user concerned has given consent to the processing of communications metadata for one or more specified purposes; or</p> <p>(d) it is necessary in order to protect the vital interest of a natural person; or</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>(e) in relation to metadata that constitute location data, it is necessary for scientific or historical research purposes or statistical purposes, provided that:</p> <ul style="list-style-type: none"> i. such data is pseudonymised; 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 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. <p>(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.</p> <p>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 and in accordance, respectively, with</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>national or Union law.</p> <p>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.</p>
		<p><i>Article 6c [Previous art 6(2a)] Compatible processing of electronic communications metadata</i></p> <p>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 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, <i>inter alia</i>:</p> <p>(a) any link between the purposes for which the electronic communications metadata have been collected and the purposes of the intended further processing;</p> <p>(b) the context in which the electronic</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>communications metadata have been collected, in particular regarding the relationship between end-users concerned and the provider;</p> <p>(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;</p> <p>(d) the possible consequences of the intended further processing for end-users;</p> <p>(e) the existence of appropriate safeguards, such as encryption and pseudonymisation.</p> <p>2. Such processing, if considered compatible, may only take place, provided that:</p> <p>(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</p> <p>(b) the processing is limited to electronic communications metadata that is pseudonymised, and</p> <p>(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</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>similarly significantly affects him or her.</p> <p>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.</p>
		<p>Article 6d – Processing of electronic communications data for the purpose of preventing child sexual abuse</p>
<p>Article 7 - Storage and erasure of electronic communications data</p>		
<p>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.</p>	<p>1. Without prejudice to Article 6(1b) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content, when it is no longer necessary for the provision of such service, as requested by the user. Such data may be recorded or stored by the users or by a third party entrusted by them to record, store or otherwise process such data. The user may process the data in accordance with Regulation (EU) 2016/679.</p>	<p>1. The provider of the electronic communications service shall erase electronic communications content or make that data anonymous when it is no longer necessary for the purpose of processing in accordance to article 6 (1) and 6a (1).</p>
<p>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.</p>	<p>2. Without prejudice to Article 6(1b) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer necessary for the provision of such service, as requested by the user.</p>	<p>2. Without prejudice to points (b), (c) and (d) of Article 6 (1), points (c), (d), (e), (f), point (g) of Article 6b, Article 6c and points (b) to (g) of Article 8 (1) the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer</p>

EU-Kommission	EU-Parlament	EU-Rat
		needed for the purpose of providing an electronic communication service.
<p>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.</p>	<p>3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), strictly necessary metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.</p>	<p>3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6b (1), 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.</p> <p>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 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.</p>
<p>Article 8 - Protection of information stored in and related to <i>end-users'</i> terminal equipment</p>	<p>Article 8 - Protection of information <i>transmitted to</i>, stored in and related to <i>processed by and collected from users'</i> terminal equipment</p>	<p>Article 8 - Protection of <i>end-users'</i> terminal equipment information</p>
<p>1. The use of processing and storage capabilities of</p>	<p>1. The use of processing and storage capabilities of</p>	<p>- <i>unverändert / not changend</i> -</p>

EU-Kommission	EU-Parlament	EU-Rat
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:	terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the user concerned shall be prohibited, except on the following grounds:	
<p>(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or</p> <p>(b) the end-user has given his or her consent; or</p> <p>(c) it is necessary for providing an information society service requested by the end-user; or</p> <p>(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.</p>	<p>(a) it is strictly necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or</p> <p>(b) the user has given his or her specific consent; or</p> <p>(c) it is strictly technically necessary for providing an information society service specifically requested by the user; or</p> <p>(d) if it is technically necessary for measuring the reach of an information society service requested by the user, provided that such measurement is carried out by the provider, or on behalf of the provider, or by a web analytics agency acting in the public interest including for scientific purpose; that the data is aggregated and the user is given a possibility to object; and further provided that no personal data is made accessible to any third party and that such measurement does not adversely affect the fundamental rights of the user; Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of</p>	<p>(a) it is necessary for the sole purpose of providing an electronic communication service; or</p> <p>(b) the end-user has given consent; or</p> <p>(c) it is strictly necessary for providing a service specifically requested by the end-user; or</p> <p>(d) if it is necessary for the sole purpose of audience measuring, provided that such measurement is carried out by the provider of the service requested by the end-user, 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</p>

EU-Kommission	EU-Parlament	EU-Rat
	<i>audience measuring on behalf of other providers; or</i>	
	<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><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><i>(ii) the user is informed in advance each time an update is being installed; and</i></p> <p><i>(iii) the user has the possibility to postpone or turn off the automatic installation of these updates;</i></p> <p><i>(d b) in the context of employment relationships, it is strictly technically necessary for the execution of an employee's task, where:</i></p> <p><i>(i) the employer provides and/or is the user of the terminal equipment;</i></p> <p><i>(ii) the employee is the user of the terminal equipment;</i></p> <p><i>and</i></p> <p><i>(iii) it is not further used for monitoring the employee.</i></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 (e) it is necessary for a software update provided that: (i) such update is necessary for security reasons and does not in any way change the privacy settings chosen by the end-user, (ii) the end-user is informed in advance each time an update is being installed, and (iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or</i></p> <p><i>(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).</i></p> <p><i>(g) where the processing for 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-</i></p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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:</p> <ul style="list-style-type: none"> (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; (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; (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; (iv) the possible consequences of the intended further processing for end-users; (v) the existence of appropriate safeguards, such as encryption and pseudonymisation. <p>(h) Such further processing in accordance with</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>paragraph 1 (g), if considered compatible, may only take place, provided that:</p> <ul style="list-style-type: none"> (i) the information is erased or made anonymous as soon as it is no longer needed to fulfil the purpose, (ii) the processing is limited to information that is pseudonymised, and (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. <p>(i) For the purposes of paragraph 1 (g) and (h), data shall not be 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.</p>
	<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>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,</p>	<p>2. The processing of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited,</p>	<p>2. The collection of information emitted by terminal equipment of the end-user to enable it to connect to another device and, or to network equipment shall be</p>

EU-Kommission	EU-Parlament	EU-Rat
except if:	except if:	prohibited, except on the following grounds:
(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or	(a) it is done exclusively in order to, for the time necessary for, and for the sole purpose of establishing a connection requested by the user ; or	(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing or maintaining a connection; or
	(aa) the user has been informed and has given consent; or (ab) the risks are mitigated.	
(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.	- gelöscht / deleted -	(b) the end-user has given consent; or (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, (d) it is necessary for providing a service requested by the end-user.
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.	- gelöscht / deleted -	
	2a. For the purpose of points (d) of paragraph 1 and (ab) of paragraph 2, the following controls shall be implemented to mitigate the risks: (a) the purpose of the data collection from the terminal equipment shall be restricted to mere statistical	2a. For the purpose of paragraph 2 points (b) and (c), a clear and prominent notice is-shall be 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-Kommission	EU-Parlament	EU-Rat
	<p><i>counting; and</i></p> <p><i>(b) the processing shall be limited in time and space to the extent strictly necessary for this purpose; and</i></p> <p><i>(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and</i></p> <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>(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.</p>
	<p>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.</p>	<p>2b. 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.</p>
<p>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.</p>	<p>3. The information to be provided pursuant to paragraph 2b 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.</p>	<p>3. The information to be provided pursuant to paragraph 2a 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.</p>
		<p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 25</p>

EU-Kommission	EU-Parlament	EU-Rat
		determining the information to be presented by the standardized icon and the procedures for providing standardized icons.
Article 9 - Consent		- gelöscht / deleted -
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 in Regulation (EU) 2016/679/EU shall apply.	- gelöscht / deleted -
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 or withdrawn by using technical specifications for electronic communications services or information society services which allow for specific consent for specific purposes and with regard to specific service providers actively selected by the user in each case, pursuant to paragraph 1. When such technical specifications are used by the user's terminal equipment or the software running on it, they may signal the user's choice based on previous active selections by him or her. These signals shall be binding on, and enforceable against, any other party.	- gelöscht / deleted -
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	3. Users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3), point (b) of Article 8(1) and point (aa) of Article 8(2) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU)	- gelöscht / deleted -

EU-Kommission	EU-Parlament	EU-Rat
<i>periodic intervals of 6 months</i> , as long as the processing continues.	2016/679 as long as the processing continues.	
	3 a. Any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communication, in particular their rights to privacy and the protection of personal data.	
Article 10 - Information and options for privacy settings to be provided		- gelöscht / deleted -
1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.	1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall: (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); (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); (c) offer the user the possibility to express specific	- gelöscht / deleted -

EU-Kommission	EU-Parlament	EU-Rat
	<i>consent through the settings after the installation of the software.</i>	
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.	<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>	<i>- gelöscht / deleted -</i>
	<i>1a. For the purpose of: (a) points (a) and (b) of paragraph 1, (b) giving or withdrawing consent pursuant to Article 9(2) of this Regulation, and (c) objecting to the processing of personal data pursuant to Article 21(5) of Regulation (EU) 2017/679, 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>	
	<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</i>	

EU-Kommission	EU-Parlament	EU-Rat
	<i>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>	
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 <i>[xx.xx.xxxx]</i> , the requirements under paragraphs 1, 1a and 1b shall be complied with at the time of the first update of the software, but no later than six months after [the date of entry into force of this Regulation] .	- gelöscht / deleted -
Article 11 Restrictions	- gelöscht / deleted -	- unverändert / not changend -
1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.	- gelöscht / deleted -	1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1) (c) to (e), (i) and (j) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. 1a. Article 23 (2) of Regulation (EU) 2016/679 shall apply to any legislative measures referred to in

EU-Kommission	EU-Parlament	EU-Rat
		paragraph 1.
<p><i>2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.</i></p>	<p>- gelöscht / deleted -</p>	<p>- unverändert / not changend -</p>
	<p>Article 11a -Restrictions on the rights of the user</p>	
	<p><i>1. Union or Member State law to which the provider is subject may restrict by way of a legislative measure the scope of the obligations and principles relating to processing of electronic communications data provided for in Articles 6, 7 and 8 of this Regulation in so far as its provisions correspond to the rights and obligations provided for in Regulation (EU) 2016/679, when such a restriction fully respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (d) of Regulation (EU) 2016/679.</i></p> <p><i>2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least,</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<i>where relevant, pursuant to Article 23(2) of Regulation (EU) 2016/679.</i>	
	Article 11b - Restrictions on confidentiality of communications	
	<p><i>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><i>(a) national security;</i></p> <p><i>(b) defence;</i></p> <p><i>(c) public security;</i></p> <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><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>	
	Article 11 c - Documentation and reporting of restrictions	

EU-Kommission	EU-Parlament	EU-Rat
	<p>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:</p> <ul style="list-style-type: none"> (a) the in-house staff member who handled the request; (b) the identity of the body making the request; (c) the purpose for which the information was sought; (d) the date and time of the request; (e) the legal basis and authority for the request, including the identity and status or function of the official submitting the request; (f) the judicial authorisation of the request; (g) the number of users to whose data the request related; (h) the data provided to the requesting authority; and (i) the period covered by the data. <p>The documentation shall be made available to the competent supervisory authority upon request.</p> <p>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:</p> <ul style="list-style-type: none"> (a) the number of requests; (b) the categories of purposes for the request; (c) the categories of data requested; 	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>(d) the legal basis and authority for the request;</i> <i>(e) the number of users to whose data the request related;</i> <i>(f) the period covered by the data;</i> <i>(g) the number of negative and positive responses to those requests.</i></p> <p>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:</p> <p><i>(a) the number of requests;</i> <i>(b) the categories of purposes for the request;</i> <i>(c) the categories of data requested;</i> <i>(d) the legal basis and authority for the request;</i> <i>(e) the number of users to whose data the request related;</i> <i>(f) the period covered by the data;</i> <i>(g) the number of negative and positive responses to those requests.</i></p> <p><i>The reports shall also contain statistical information per month about any other restrictions pursuant to Articles 11a and 11b.</i></p>	
CHAPTER III - NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS		CHAPTER III <i>END-USERS'</i> RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS

EU-Kommission	EU-Parlament	EU-Rat
Article 12 - Presentation and restriction of calling and connected line identification		
<p>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:</p> <p>(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;</p> <p>(b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;</p> <p>(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;</p> <p>(d) the called end-user with the possibility of preventing the presentation of the connected line identification to the calling end-user.</p>	<p>- <i>unverändert / not changend</i> -</p>	<p>1. Where presentation of the calling and connected line identification is offered in accordance with Article [115] of the Directive (EU) 2018/1972, the providers of number-based interpersonal communications services shall provide the following:</p> <p>(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;</p> <p>(b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;</p> <p>(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;</p> <p>(d) the called end-user with the possibility of preventing the presentation of the connected line identification to which the calling end-user is connected.</p>
<p>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.</p>	<p>- <i>unverändert / not changend</i> -</p>	<p>2. The possibilities referred to in paragraph 1 shall be provided to end-users by simple means and free of charge.</p>
<p>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 shall also apply to incoming calls originating in third countries.</p>		

EU-Kommission	EU-Parlament	EU-Rat
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.	- <i>unverändert / not changend</i> -	4. Where presentation of calling or connected line identification is offered, providers of number-based interpersonal communications services shall provide information to the public regarding the options set out in paragraph 1 and the exceptions set forth in Article 13.
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 <i>in relation to emergency communications</i>
1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.	1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of a user for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications	1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where emergency communications are made to emergency services, providers of 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.
		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,

EU-Kommission	EU-Parlament	EU-Rat
		<p>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.</p>
<p>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.</p>	<p>2. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(1) 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 users request the tracing of malicious or nuisance calls.</p>	<p>- gelöscht / deleted -</p>
		<p>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 settings may not prevent access to GNSS-such location data to determine and provide the callercalling end-user's location to emergency servicesan organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such calls.</p>

EU-Kommission	EU-Parlament	EU-Rat
Article 14 - Incoming call blocking		Article 14 Blocking <i>Unwanted, malicious or nuisance calls</i>
<p>Providers of publicly available number-based interpersonal communications services <i>shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also</i> provide the called end-user with the following possibilities, free of charge:</p> <p>(a) to block incoming calls from specific numbers or from anonymous sources;</p> <p>(b) to stop automatic call forwarding by a third party to the <i>end-user's</i> terminal equipment.</p>	<p>Providers of publicly available number-based interpersonal communications services provide the called end-user with the following possibilities, free of charge:</p> <p>(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;</p> <p>(b) to stop automatic call forwarding by a third party to the <i>user's</i> terminal equipment.</p>	<p>1. Providers of number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted, malicious or nuisance calls by end-users.</p> <p>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.</p> <p>2. Providers of number-based interpersonal communications services shall also provide the called end-user with the following possibilities, free of charge:</p> <p>(a) to block, where technically feasible, incoming calls from specific numbers or from anonymous sources or from numbers using a specific code or prefix referred to in Article 16(3a); and</p> <p>(b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.</p>
Article 15 - Publicly available directories		
1. <i>The</i> providers <i>of publicly available directories</i> shall	1. <i>Without prejudice to Articles 12 to 22 of Regulation</i>	1. The providers of number-based interpersonal

EU-Kommission	EU-Parlament	EU-Rat
<p>obtain the consent of <i>end-users who are natural persons</i> to include their personal data in the directory and, consequently, shall obtain consent from these <i>end-users</i> for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory <i>as determined by the provider of the directory.</i> Providers shall give <i>end-users who are natural persons</i> the means to verify, correct and delete such data.</p>	<p><i>(EU) 2016/679, the electronic communication services</i> providers shall obtain the consent of <i>users</i> to include their personal data in the <i>publicly available</i> directory and, consequently, shall obtain consent from these <i>users</i> for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory. <i>Electronic communication service</i> providers shall give <i>users</i> the means to verify, correct, <i>update, supplement</i> and delete such data. <i>When electronic communication service providers obtain consent of users, they shall make users' data available for public directory providers in an immediate, non-discriminatory and fair manner.</i></p>	<p>communications services shall obtain the consent of end-users who are natural persons to include their personal data in the directory and for inclusion of such 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.</p> <p>1aa. 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 he end-user who is a natural person shall have the right to object to such inclusion.</p>
<p>2. The providers of a publicly available directory shall inform <i>end-users who are natural persons</i> whose personal data are in the directory of the available search functions of the directory and <i>obtain end-users' consent before enabling</i> such search functions related to their own data.</p>	<p>2. The providers of a publicly available directory shall inform <i>users</i> whose personal data are in the directory of the available search functions of the directory and <i>provide the users the option to disable</i> such search functions related to their own data.</p>	<p>2. The providers of number-based interpersonal communications services shall inform end-users who are natural persons whose personal data are in the directory of any search functions that is not based on name or number in the directory and obtain the consent of end-users' before enabling such search functions related to their own data.</p>
<p>3. The providers <i>of publicly available directories</i> 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.</p>	<p>3. The <i>electronic communication service</i> providers shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. <i>Electronic communication service</i> providers shall give such end-users that are legal persons the means to verify, correct and delete</p>	<p>3. The providers of number-based interpersonal communications services shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory.</p> <p>3a. The providers of number-based interpersonal communications services shall give end-users the</p>

EU-Kommission	EU-Parlament	EU-Rat
	such data. <i>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.</i>	means to verify, correct and delete data included in a publicly available directory. 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.
4. The possibility <i>for end-users</i> 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. <i>Without prejudice to Article 12(5) of Regulation (EU) 2016/679, the information to the users and</i> the possibility not to be included in a publicly available directory, or to verify, correct, <i>update, supplement</i> and delete any data related to them shall be provided free of charge <i>and in an easily accessible manner by the electronic communication services providers.</i>	- <i>unverändert / not changend</i> -
	<i>4 a. Where the personal data of the users of number-based interpersonal communications services have been included in a publicly available directory before this Regulation enters into force, the personal data of such users may remain included in a publicly available directory, including versions with search functions, unless the users have expressed their objection against their data being included in the directory or against available search functions related to their data.</i>	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.
Article 16 - Unsolicited communications		Article 16 - Unsolicited <i>and direct marketing</i>

EU-Kommission	EU-Parlament	EU-Rat
<p>1. Natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons that have given their consent.</p>	<p>1. The use by natural or legal persons of electronic communications services, including automated calling, communications systems, semi-automated systems that connect the call person to an individual, faxes, e-mail or other use of electronic communications services for the purposes of presenting or sending direct marketing communications to users, shall be allowed only in respect of users who have given their prior consent.</p>	<p style="text-align: center;">communications</p> <p>1. Natural or legal persons shall be prohibited from using electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons unless they have given their prior consent.</p>
<p>2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.</p>	<p>2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The customer shall be informed about the right to object and shall be given an easy way to exercise it at the time of collection and each time a message is sent.</p>	<p>2. Notwithstanding paragraph 1, where a natural or legal person obtains contact details for electronic message from end-users who are natural persons, in the context of the purchase of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these contact details for direct marketing of its own similar products or services only if such end-users 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 of such end-users' contact details and, if that end-user has not initially refused that use, each time when a natural or legal persons sends a message to that end-user for the purpose of such direct marketing.</p>
		<p>2a. Member States may provide by law a set period of time, after the sale of the product or service occurred,</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>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.</p>
<p>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:</p> <p>(a) present the identity of a line on which they can be contacted; or</p> <p>(b) present a specific code/or prefix identifying the fact that the call is a marketing call.</p>	<p>- unverändert / not changend -</p>	<p>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.</p>
	<p><i>3 a. The masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited communications for direct marketing purposes is prohibited.</i></p>	<p>3a. Member States may require natural or legal person using electronic communications 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.</p>
<p>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</p>	<p>4. Notwithstanding paragraph 1, the placing of direct marketing voice-to-voice calls to users shall only be allowed in respect of users who have not expressed their objection to receiving those communications. Member States shall provide that users can object to</p>	<p>- unverändert / not changend -</p>

EU-Kommission	EU-Parlament	EU-Rat
objection to receiving those communications.	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.	
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.	- unverändert / not changend -	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 direct marketing communications sent by means set forth under paragraph 1 are sufficiently protected.
6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications.	6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner and free of charge , to receiving further marketing communications.	6. Any natural or legal person using electronic communications services to send direct marketing communications shall, each time a direct marketing communication is sent: (a) reveal his or its identity and use effective return addresses or numbers; (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; (c) (d) 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

EU-Kommission	EU-Parlament	EU-Rat
		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.
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 26(1) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.	- gelöscht / deleted -
Article 17 - Information about detected security risks		- gelöscht / deleted -
<i>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.</i>	(1) Providers of electronic communications services shall comply with the security obligations as prescribed Regulation (EU) 2016/679 and [European Electronic Communications Code]. As regards the security of networks and services and related security obligations, the obligations of Article 40 of the [European Electronic Communications Code] shall apply mutatis mutandis to all services in the scope of this Regulation. This Article shall be without prejudice to the obligations provided for in Articles 32 to 34 of Regulation (EU) 2016/679 and the obligations provided for in Directive (EU) 2016/1148.	- gelöscht / deleted -
	(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	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>cryptographic methods including end-to-end encryption of the electronic communications data. When encryption of electronic communications data is used, decryption by anybody else than the user shall be prohibited. Notwithstanding Articles 11a and 11b of this Regulation, member States shall not impose any obligations on electronic communications service providers or software manufacturers that would result in the weakening of the confidentiality and integrity of their networks and services or the terminal equipment, including the encryption methods used.</i></p>	
	<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 communications. Notwithstanding Articles 11a and 11b of this Regulation, breaking, decrypting, restricting or circumventing such measure taken by users or subscribers shall be prohibited.</i></p>	
	<p><i>(1c) In the case of a particular risk that may compromise the security of networks, electronic communications</i></p>	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>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></p>	
<p>CHAPTER IV - INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT</p>		
<p>Article 18 - Independent supervisory authorities</p>		<p>Article 18 - Supervisory authorities</p>
		<p>0. 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. 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.</p>
<p>1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the</p>	<p>1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. Where Regulation (EU)</p>	<p><i>- gelöscht / deleted -</i></p>

EU-Kommission	EU-Parlament	EU-Rat
<p>supervisory authorities shall be exercised with regard to end-users.</p>	<p>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.</p>	
		<p>1ab. The supervisory authorities shall have investigative and corrective powers, including the power to impose administrative fines pursuant to article 23.</p> <p>1b. Where more than one supervisory authority is responsible for monitoring the application of this Regulation in a Member State, such authorities shall cooperate with each other to the extent necessary to perform their tasks.</p>
<p>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].</p>	<p>- unverändert / not changend -</p>	<p>2. Where the supervisory authorities are not the supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679, they shall cooperate with the latter and, whenever appropriate, with national regulatory authorities established pursuant to Directive (EU) 2018/1972 and other relevant authorities.</p>
<p>Article 19 - European Data Protection Board</p>		

EU-Kommission	EU-Parlament	EU-Rat
<p>The European Data Protection Board, established under Article 68 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:</p> <p>(a) advise the Commission on any proposed amendment of this Regulation;</p> <p>(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 in order to encourage consistent application of this Regulation.</p>	<p>- <i>unverändert / not changend</i> -</p>	<p>1. The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have the task to contribute to the consistent application of Chapters I and II and III of this Regulation.</p> <p>2. To that end, the Board shall have the following tasks:</p> <p>(a) advise the Commission on any proposed amendment of this Regulation; (b) examine, on its own initiative, on request of a supervisory authority designated in accordance with Article 18 (0) or on request of the Commission, any question covering the application of this Regulation in relation to Chapters I, II and III and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;</p>
	<p><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></p>	<p>(c)</p>
	<p><i>(bb) issue guidelines to determine which technical specifications and signalling methods fulfil the conditions and objectives pursuant to Article 10(1a);</i></p>	<p>(d) issue guidelines, recommendations and best practices in order to facilitate cooperation, including exchange of information, between supervisory authorities referred to in paragraph 0 of Article 18 and/or the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679;</p>
	<p><i>(bc) issue guidelines, recommendations and best</i></p>	<p>(da) issue guidelines, recommendations and best</p>

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>practices in accordance with point (b) of this paragraph for the purpose of further specifying the criteria and requirements for types of services that may be requested for purely individual or work-related usage as referred to in Article 6(3a);</i></p>	<p>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 content;</p>
	<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> <ul style="list-style-type: none"> <i>(i) measuring the reach of an information society service referred to in Article 8(1) point (d);</i> <i>(ii) security updates referred to in Article 8(1) point (da);</i> <i>(iii) the interference in the context of employment relationships referred to in Article 8(1) point (db);</i> <i>(iv) the processing of information emitted by the terminal equipment referred to in Article 8(2) ();</i> <i>(v) technical specifications and signalling methods that fulfil the conditions for consent and objection pursuant to Article 8(2a);</i> <i>(vi) software settings referred to in Article 10(1a) and (1b); and</i> <i>(vii) technical measures to ensure confidentiality and integrity of the communication pursuant to Article 17(1a), (1b) and (1c).</i> 	<p>(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 and or in an employment relationship; (e) provide the Commission with an opinion on the icons referred to in paragraph 3 of Article 8;</p> <p>(f)</p> <p>(g)</p> <p>(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;</p>
		<p>3. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account</p>

EU-Kommission	EU-Parlament	EU-Rat
		<p>the urgency of the matter.</p> <p>4. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and make them public.</p> <p>5. The Board shall consult the supervisory authorities referred to in Article 18 (0) before any of the tasks referred to in paragraph 2.</p> <p>6. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76 of Regulation (EU) 2016/679, make the result of the consultation procedures publicly available.</p>
Article 20 - Cooperation and consistency procedures		Article 20 - Cross-border cooperation
<p>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.</p>		<p>Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union and cooperate with each other and with the Commission.</p>
CHAPTER V - REMEDIES, LIABILITY AND PENALTIES		
Article 21 - Remedies		
<p>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.</p>	<p>1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services and, where applicable, every body, organisation or association, shall have the same remedies provided for in Articles 77, 78, 79 and 80 of</p>	<p>1. Without prejudice to any other administrative or judicial remedy, every end-user 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</p>

EU-Kommission	EU-Parlament	EU-Rat
	Regulation (EU) 2016/679.	the right to an effective judicial remedy against any legally binding decision of a supervisory authority concerning them.
	<i>1 a. Without prejudice to any other administrative or non-judicial remedy, every end-user of electronic communications services shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him or her. End-users shall also have such a right where the supervisory authority does not handle a complaint or does not inform the end- user within three months on the progress or outcome of the complaint lodged. Proceedings against a supervisory authority shall be brought before the court of the Member State where the supervisory authority is established.</i>	1a Articles 77-80 of Regulation (EU) 2016/679 shall apply <i>mutatis mutandis</i>.
	<i>1 b. Every end-user of the communications services shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed. Those proceedings against a provider of electronic communication service, the provider of a publicly available directory, software provider enabling electronic communication or persons sending direct marketing commercial communications or collecting information related to or stored in the end-users terminal equipment shall be brought before the courts of the Member State where they have an</i>	

EU-Kommission	EU-Parlament	EU-Rat
	<i>establishment. Alternatively, such proceedings shall be brought before the court of the Member State of the habitual residence of the end-user.</i>	
2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation <i>and having a legitimate interest in the cessation or prohibition of alleged infringements</i> , 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, 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 - Right to compensation and liability		
Any <i>end-user</i> 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 person 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 in accordance with Article 82 of Regulation (EU) 2016/679.
Article 23 - General conditions for imposing administrative fines		
1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation.	1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation, <i>mutatis mutandis</i> .	1. Article 83 of Regulation (EU) 2016/679 shall apply <i>mutatis mutandis</i> to infringements of this Regulation.
2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial	- <i>unverändert / not changed</i> -	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

EU-Kommission	EU-Parlament	EU-Rat
year, whichever is higher:		year, whichever is higher:
(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;	- gelöscht / deleted -	(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;
	(a a) the obligations of the providers of electronic communications services pursuant to Article 11c;	
(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;	- gelöscht / deleted -	- gelöscht / deleted -
	(b a) the obligations of the providers of publicly available number-based interpersonal communication services pursuant to Articles 12, 13 and 14.	
(c)the obligations of the providers of publicly available directories pursuant to Article 15;		
(d)the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.		
		(e) the obligation to designate a representative pursuant to Article 3 number 2.
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 following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:	- unverändert / not changend -
	(a) the principle of confidentiality of communications	

EU-Kommission	EU-Parlament	EU-Rat
	<p><i>pursuant to Article 5;</i></p> <p><i>b) the permitted processing of electronic communications data, pursuant to Article 6;</i></p> <p><i>(c) the time limits for erasure and the confidentiality obligations pursuant to Article 7;</i></p> <p><i>(d) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;</i></p> <p><i>(e) the requirements for consent pursuant to Article 9;</i></p> <p><i>(f) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;</i></p> <p><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></p>	
<p>4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17.</p>	<p>4. In the event that the same act or omission by the same person results in non-compliance with both Regulation (EU) 2016/679 and this Regulation, then the maximum administrative fine shall be no more than the maximum administrative fine applicable under this Regulation for that type of infringement.</p>	<p>4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13 and 14.</p>
<p>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.</p> <p>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.</p>		

EU-Kommission	EU-Parlament	EU-Rat
<p>7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.</p> <p>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.</p>		
<p>Article 24 - Penalties</p>		
<p>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.</p> <p>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.</p>		
<p>CHAPTER VI - DELEGATED ACTS AND IMPLEMENTING ACTS</p> <p>Article 25 - Exercise of the delegation</p>		
<p>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</p> <p>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 date of entering into force of this Regulation].</p> <p>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.</p> <p>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.</p> <p>5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p> <p>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</p>		

EU-Kommission	EU-Parlament	EU-Rat
<p>period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.</p>		
<p>Article 26 - Committee</p>		
<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</p>	<p>1. For the purpose of Articles 13(2) and 16(7), the Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011</p>	<p>1. The Commission shall be assisted by the Communications Committee established under Article 118 of Directive (EU) 2018/1972. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011-</p>
<p>2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.</p>		
<p>CHAPTER VII - FINAL PROVISIONS</p>		
<p>Article 27 - Repeal</p>		
<p>1. Directive 2002/58/EC is repealed with effect from 25 May 2018.</p>	<p>1. Directive 2002/58/EC and Commission Regulation 611/2013 are repealed with effect from [XXX]</p>	<p>1. Directive 2002/58/EC is repealed with effect from [1 August 2022].</p>
<p>2. References to the repealed Directive shall be construed as references to this Regulation.</p>		
<p>Article 28 - Monitoring and evaluation clause</p>		
<p>By 1 January 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.</p>	<p>By [the date of entry into force of this Regulation] at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation</p>	<p>By [1 August 2024] at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.</p>
<p>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</p>		

EU-Kommission	EU-Parlament	EU-Rat
a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.		
Article 29 - Entry into force and application		
1.This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.		
2.It shall apply from 25 May 2018.	2. It shall apply from <i>[one year the date of entry into force of this Regulation].</i>	2. This Regulation shall apply from [24 months from the date of entry into force of this Regulation].