

Brussels, 6 March 2020
(OR. en)

6543/20

Interinstitutional File:
2017/0003(COD)

TELECOM 30
COMPET 102
MI 59
DATAPROTECT 28
CONSOM 42
JAI 212
DIGIT 12
FREMP 20
CYBER 32
CODEC 152

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	5979/20
No. Cion doc.:	5358/17
Subject:	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)

1. In view of the WP TELE meetings of 12 and 19 March, delegations will find in Annex a consolidated text of the ePrivacy proposal. The text includes the modifications to articles 6 to 8 and the related recitals as introduced by the previous Presidency document (doc. 5979/20) and certain new modifications with regard to **the scope and M2M and IoT services**.
2. The **modifications** introduced by the present document are marked in underline and listed below:
 - the Presidency has deleted the reference to 'third parties' in **art. 2(2)(e)** as well as the entire **art. 2(2)(f)**. The Presidency has tried to address the issues tackled by those text parts in new **recital 8aa**;

- further clarifications have been introduced in **recital 12** with regard to M2M and Internet of Things services;

- the Presidency has also continued the efforts to improve the text by grouping various recital parts relating to the same topic, mostly without changes in substance. This would concern in particular moving text parts between **recitals 8aa, 15a, 16a, 16b, 16c, 19, 19a and 19b** and deleting the remaining part of **recital 19**.

3. During the **meeting of 12 March**, the Presidency would like to:

- discuss in detail modifications to articles 6 to 8 and the related recitals;

- if time allows, examine the modifications related to the scope and M2M and IoT services.

The discussion on the proposal will most likely continue on **19 March**. The Presidency will decide on the precise agenda on the basis of the outcome of the meeting of 12 March.

4. As announced during the WP TELE meeting of 5 March, the Presidency would like to invite delegations to provide their **written comment in relation to articles 6 to 8 by 10 March**.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee¹,

Having regard to the opinion of the Committee of the Regions²,

Having regard to the opinion of the European Data Protection Supervisor³,

Acting in accordance with the ordinary legislative procedure,

Whereas:

¹ OJ C , , p. .

² OJ C , , p. .

³ OJ C , , p. .

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

(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. 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

- (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 Council⁴, also apply *mutatis mutandis* to end-users who are legal persons. This includes the ~~definition of~~ **provisions on** consent under Regulation (EU) 2016/679. ~~When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.~~
- (3a) **This Regulation should not affect national law regulating for instance the conclusion or the validity of a contract. Similarly, this Regulation should not affect national law in relation to determining who has the legal power to represent legal persons in any dealings with third parties or in legal proceedings.**
- (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 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

- (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.~~
- (6) While the principles and main provisions of Directive 2002/58/EC of the European Parliament and of the Council⁵ remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. Those developments include the entrance on the market of electronic communications services that from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules. Another development concerns new techniques that allow for tracking of online behaviour of end-users, which are not covered by Directive 2002/58/EC. Directive 2002/58/EC should therefore be repealed and replaced by this Regulation.

⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

- (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.
- (7a) **This Regulation should 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 activities concerning national security and defence.**
- (8) This Regulation should apply to providers of electronic communications services; and 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 **make use of processing and storage capabilities of terminal equipment or** collect information ~~related to~~ **processed by or emitted by** or stored in end-users' terminal equipment. **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.**

(8aa) End-users, including legal entities, should be allowed to process their electronic communications data as from receipt and are free to use a third party to process their electronic communications data on their behalf. The relationship between the end-user and the third party, including regarding the use of the end-user's electronic communications data, is governed by Regulation (EU) 2016/679. Some end-users, fFor example end-users, including providers of payment services or payment systems or information society services, 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, should have the possibility to take the necessary measures to secure process their own electronic communications data to protect 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 e-sphere. For example, aAn end-user as an information society service provider may process its electronic communications data, or may request could also mandate a third party, such as a provider of security technologies and services, to process that end-user's electronic communications data as from receipt on its behalf, for the purposes such as of ensuring that end-user's 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 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. This should not prevent could include processing of electronic communications data on the end-user's terminal equipment or within or at the edge of the end-user's closed network – even before receipt – by third parties mandated by the end-user for the purpose of protecting the that end-user's terminal equipment or closed network.

Consequently, once the electronic communications data has arrived at the edge of the end-user's closed network or terminal equipment, it could be processed in a way that is effective for the purpose of protecting the closed network or terminal equipment.

In this context, aA third party should refer to a legal or natural person that does not provide an electronic communications service to the end-user concerned. However, sometimes the same legal or natural person could also provide different kind of other services to the same end-user, for example information society service such as cloud storage or network and information security services. With respect to the provision of this those other services, the same that legal and natural person should be considered as a third party, unless. 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 should not be deemed to be a third party.

(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.

~~(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.~~

(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 Council⁶. 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.

⁶ Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).

(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 of the European Parliament and of the Council establishing the European Electronic Communications Code⁷}~~. 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.

(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 also having a communication functionality~~ should be covered by this Regulation.

⁷ **Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).** ~~Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final – 2016/0288 (COD)).~~

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 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.

- (12) ~~Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). 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, it is necessary to clarify that this Regulation, in particular the requirements relating to the confidentiality of communications, should apply to the transmission of machine-to-machine electronic communications where carried out via an publicly available electronic communications such services. The transmission services used for the provision of machine-to-machine or Internet of Things services regularly involves the conveyance of signals via an electronic communications network and, hence, constitutes an electronic communications service. This Regulation should apply to the provider of the transmission service if that transmission is carried out via a publicly available electronic communications service or network. While 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. the services provided at the application layer of machine-to-machine such services do normally not qualify as an electronic communications service as defined in Directive (EU) 2018/1972, Tthe transmission services used for the provision of machine-to-machine communications services regularly involves the conveyance of signals over via an electronic communications network and, hence, usually constitutes an electronic communications service. Typically, providers of machine-to-machine or Internet of Things services operate at the application layer (on top of electronic communications services). and thus they or These service providers and their customers who use IoT devices 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. 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, in particular the requirements relating to the confidentiality of communications, should~~

~~apply to the transmission of machine-to-machine **electronic** communications **where carried out via an publicly available electronic communications service**.~~ Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.

(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 passwords or not**, 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 **publicly available** electronic communications services and public **electronic** communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as **home (fixed or wireless) networks or corporate networks or networks to which the access to which is limited to a pre-defined group of end-users, e.g. to family members or members of the a corporation.** 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' 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 public electronic communications network.

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

- (15) Electronic communications data should be treated as confidential. This means that any interference ~~with the transmission~~ of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of ~~all~~ the communicating parties should be prohibited. ~~The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee.~~

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

(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. Moreover, trade secrets are protected in accordance with Directive (EU) 2016/943.

(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 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 ~~or when the end-users has entrusted a third party to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679. This should not prevent processing of electronic communications data on the end-user's terminal equipment or within the end-user's closed network—even before receipt—by third parties mandated by the end-user for the purpose of protecting the end-user's terminal equipment or closed network.~~ 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, ~~or by a third party entrusted by them to record or store such data as this kind of processing is outside of the scope of this Regulation~~ End-users are free to mandate a third party to record or store such data on their behalf.

(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 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 ~~either~~ the processing of electronic communications data **without consent of the end-user** to ensure the security ~~and continuity~~, **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. ~~Moreover, the prohibition of processing should neither prohibit the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc., nor the processing of metadata necessary for the purpose of management or optimisation of the network. Management or optimisation of the network refers to processing necessary to develop and manage the scalability and capacity of the network. The processing of data to make it anonymous should not be prohibited either.~~

(16a9) The **protection of the** content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications ~~data~~ **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 ~~data~~ **content**, the provider of the electronic communications service should ~~always~~ consult the supervisory authority ~~prior to the processing~~ **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 ~~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.

(16b9a) 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.

(16c9b) Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal person having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service in accordance with Regulation 2016/679.

- (17) The processing of electronic communications **metadata** can be useful for businesses, consumers and society as a whole. Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, ~~based on end-users consent~~. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and ~~that~~ they **also** want to control the use of electronic communications **metadata** for purposes other than conveying the communication. Therefore, ~~this Regulation should require providers of electronic communications networks and services should be permitted to process electronic communications metadata after having obtained to obtain the end-users' consent to process electronic communications metadata, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata. 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. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.~~

~~(17aa) Metadata such as location data can provide valuable information, such as insights in human movement patterns and traffic patterns. Such information may, for example, be used for urban planning purposes. Further processing for such purposes other than for which the metadata were initially collected may take place without the consent of the end-users concerned, provided that such processing is compatible with the purpose for which the metadata are initially collected, certain additional conditions are met and safeguards are in place, including, where appropriate, the consultation of the supervisory authority, an impact assessment by the provider of electronic communications networks and services and 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 of 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.~~

(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 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 protection of such interests cannot be ensured without that processing.

(17b) The legitimate interests of an electronic communications network or service provider may provide a legal basis for processing of electronic communications metadata, provided that the interests or the fundamental rights and freedoms of the end-user are not overriding, taking into consideration the reasonable expectations of the end-user based on her or his relationship with the provider. A relevant and appropriate relationship could exist where the end-user is a client of the provider. The demonstration of a legitimate interest requires careful assessment, in particular whether an end-user can reasonably expect at the time and in the context of the conclusion of the contract with the provider that her or his electronic communications metadata might be processed for that purpose. Only when the results of the assessment undertaken by the electronic communications network or service provider demonstrate that its legitimate interest is not overridden by the interests and the fundamental rights and freedoms of the end-user, can the provider rely on that legal basis. A legitimate interest of a provider of electronic communications networks or services to process electronic communications metadata could exist where such processing is necessary for the purpose of detecting or stopping fraudulent or abusive use of, or subscription to, electronic communications services, or for calculating and billing interconnection payments or for the purposes of network management or network optimisation. Management or optimisation of the network refers to processing necessary to develop and manage the scalability and capacity of the network. A legitimate interest could also consist in meeting mandatory technical quality of service requirements pursuant to Directive (EU) 2018/1972 or Regulation (EU) 2015/2120, including requirements related to latency, jitter etc. Processing of electronic communication metadata for scientific research or statistical counting purposes ~~should~~ could also be considered as a legitimate interest of the provider, for instance for the provision of heat maps, a graphical representation of data using colours to indicate the presence of individuals ~~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.~~ 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.

Conversely, as end-users attach great value to the confidentiality of their electronic communications metadata, including their physical movements, such metadata should not be used to determine the nature or characteristics of an end-user or to build an individual profile of an end-user. In such usage cases, the end-user's interests and fundamental rights and freedoms override the interest of the service provider, as such processing operations can seriously interfere with one's private life, for instance when used for segmentation purposes, to monitor the behaviour of a specific end-user or to draw conclusions concerning her or his private life. A legitimate interest also should not exist if the electronic communications metadata include special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679, unless the conditions of Article 9(2)(g) and (j) of Regulation (EU) 2016/679 are met.

- (17c) Processing of electronic communications metadata based on a legitimate interest should only be permitted subject to certain additional conditions and safeguards, namely an impact assessment, and where appropriate, the consultation of the supervisory authority, by the provider of electronic communications networks and services. In addition, the electronic communications network and service provider should not share the metadata with third parties, unless it has been previously anonymised. The electronic communications network or service providers should, where necessary, implement appropriate security measures such as encryption and pseudonymisation to ensure privacy of the end-user. Moreover, the end-user must be provided with information about these processing activities taking place and be given the right to object to such processing.**

~~(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 detriment.~~

~~(19) The **protection of the** content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data **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 data **content**, the provider of the electronic communications service should always consult the supervisory authority prior to the processing **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 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 those end-user, end-users or by a third party entrusted by them to record or store such data **as this kind of processing is outside of the scope of this Regulation**. Any processing of such data must comply with Regulation (EU) 2016/679.~~

A third party should refer to a legal or natural person that does not provide an electronic communications service to the end-user concerned. However, sometimes the same legal or natural person could 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 should be considered as 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 should not be deemed to be a third party.

(19a) 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.

(19b) Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal person having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service in accordance with Regulation 2016/679.

- (20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, ~~whether in particular where~~ **such information is stored in processed by, or emitted by or stored in, or collected from** such equipment, ~~requested 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, of the end-users requiring and require protection under 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.~~ Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, ~~any such interference with the~~ **use of processing and storage capabilities and the collection of information from** end-user's terminal equipment should be allowed only with the end-user's consent ~~and or for other~~ specific and transparent purposes **as laid down in this Regulation. The information collected from end-user's terminal equipment can often contain personal data.**

As the provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679, that Regulation should apply to the processing of this data, to the extent it is personal data, after it has been collected from the end user's terminal equipment. In light of the principle of purpose limitation according to Article 5 of Regulation (EU) 2016/679 and Article 8 of this Regulation, such data should only be processed for purposes compatible with the purpose for which it was collected from the end-user's terminal equipment.

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.

~~Making access to website content provided without direct monetary payment dependent on the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer [by the same provider] that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, 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.~~

(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 his or her 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 their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment.

- (21) ~~Exceptions to the obligation to obtain consent to make u~~Use of the processing and storage capabilities of terminal equipment or ~~to 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 ~~strictly~~ necessary and proportionate for the legitimate purpose of ~~enabling the use of~~ **providing** 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, **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 basket.** In the area of IoT services which rely ~~on/deploy~~ 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

~~In some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, such as services provided to safeguard freedom of expression and information including for journalistic purposes, such as online newspaper or other press publications as defined in Article 2(4) of Directive (EU) 2019/790, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar techniques and has accepted such use.~~

~~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 carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the service requested, consent should be required. In such a scenario, consent should normally be given by the end-user who requests the service from the provider of the service.~~

- (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 measuring web traffic to 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. 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.
- (21b) The legitimate interests of a service provider could provide a legal basis to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment, provided that such interests are not overridden by the interests or the fundamental rights and freedoms of the end-user, taking into consideration the reasonable expectations of end-user based on her or his relationship with the provider. The demonstration of a legitimate interest requires careful assessment, in particular whether an end-user can reasonably expect that the use of processing and storage capabilities of her or his terminal equipment or the collection of information from it, may take place. Only if the results of the balancing test undertaken by the service provider demonstrate that its legitimate interest is not overridden by the interests and the fundamental rights and freedoms of the end-user, can the service provider rely on that legal basis.

A legitimate interest could be relied upon where the end-user could reasonably expect such storage, processing or collection of information in or from her or his terminal equipment in the context of an existing customer relationship with the service provider. For instance, maintaining or restoring the security of information society services or of the end-user's terminal equipment, or preventing fraud or detecting technical faults might constitute a legitimate interest of the service provider.

Similarly, using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs, 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 be considered as a legitimate interest.

A legitimate interest could also be relied upon by a service provider whose website content or services are accessible without direct monetary payment and wholly or mainly financed by advertising, provided that these services safeguard the freedom of expression and information including for journalistic purposes, such as online newspaper or other press publications as defined in Article 2(4) of Directive (EU) 2019/790, or audiovisual media services as defined in Article 1(1)(a)(i) of Directive 2010/13/EU⁸ and the end-user has been provided with clear, precise and user-friendly information about the purposes of the cookies or similar techniques used and has accepted such use.

⁸ As amended by Directive (EU) 2018/1808

Conversely, a provider should not be able to rely upon legitimate interests if the storage or processing of information in the end-user's terminal equipment or the information collected from it were to be used to determine the nature or characteristics on an end-user or to build an individual profile of an end-user. In such cases, the end-user's interests and fundamental rights and freedoms override the interest of the service provider, as such processing operations can seriously interfere with one's private life, for instance when used for segmentation purposes, to monitor the behaviour of a specific end-user or to draw conclusions concerning his or her private life. A legitimate interest should not exist if the information stored or processed in, or collected from, an end-user's terminal equipment includes special categories of personal data, as referred to in Article 9 (1) of Regulation (EU) 2016/679.

~~Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs, 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.~~

- (21c) Where a service provider invokes a legitimate interest, certain additional conditions should be met and safeguards should be respected, including an impact assessment and where appropriate the consultation of the supervisory authority by the service provider. In addition, the service provider should not share the information with third parties other than its processors, in accordance with Article 28 of Regulation (EU) 2016/679, unless it has been previously anonymised. The service provider should, where necessary, implement appropriate security measures, such as encryption and pseudonymisation to ensure privacy of the end-users. Moreover, the end-user should be provided with information about these processing operations taking place and be given the right to object to such operations.

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

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

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

- (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, ~~etc~~ **referred to as statistical counting for which the consent of end-users is not needed, provided that such counting is limited in time and space to the extent necessary for this purpose. Providers should also apply appropriate technical and organisations measures to ensure the level of security appropriate to the risks, including pseudonymisation of the data and making it anonymous or erase it as soon it is not 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 **based on locations, subject to the conditions laid down in this**

Regulation, ~~While some of these functionalities do not entail high privacy risks, others do, for example, those involving as well as 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.~~

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 his or her consent or if it is necessary for the provision of a service requested by the end-user. This kind of processing might be necessary for example for the provision of some IoT related services.

- (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 ~~national security, defence~~, public security and the prevention, investigation, detection or prosecution of criminal offences, **including child sexual abuse and exploitation**, 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,

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).

- (27) As regards calling line identification, it is necessary to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. Certain end-users, in particular help lines, and similar organisations, have an interest in guaranteeing the anonymity of their callers. As regards connected line identification, it is necessary to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected.
- (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 requiring that specific categories or classes of radio equipment support certain features ensuring access to emergency services.**

- (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 ~~fraudulent~~ **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 ~~publicly available~~ number-based interpersonal communications services should deploy this technology and protect end-users against ~~nuisance such~~ 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.
- (30) ~~Publicly available directories of end-users of electronic communications services are widely distributed.~~ Publicly available directories means any directory or service containing **information on end-users information of number-based interpersonal communication services** such as **name**, phone numbers (including mobile phone numbers), email address ~~contact details~~, **home address** and includes inquiry services, **the main function of which is to enable to identify such end-users.** ~~The right to privacy and to protection of the personal data of a natural person requires that e~~End-users that are natural persons **are 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 ~~entities~~ **persons** requires that end-users that are legal ~~entities~~ **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.**

- (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, ~~p~~**Providers of publicly available directories number-based interpersonal communications services** should inform the end-users **who are natural persons** of the purposes of the directory and of the search functions of the directory **and obtain their consent** before including them in that directory **enabling such search functions related to their personal data**. ~~End-users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched.~~ The categories of personal data included in the directory and the categories of personal data on the basis of which the end-user's contact details can be searched should not necessarily be the same.
- (32) In this Regulation, direct marketing **communications** refers to any form of advertising **sent** by ~~which~~ a natural or legal person ~~sends direct marketing communications~~ directly to one or more ~~identified or identifiable~~ **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 his or her 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 this should direct marketing communications also may include messages 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 ~~should~~ **applies** to messages sent by other non-profit organisations to support the purposes of the organisation.

(33) Safeguards should be provided to protect end-users against ~~unsolicited~~ **direct marketing** communications ~~for direct marketing purposes~~, which intrude into the ~~private life~~ **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 ~~commercial electronic communications for direct marketing~~ **communications** purposes are sent to ~~end-users~~ **them** in order to effectively protect ~~individuals~~ **them** 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~~ **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 ~~unsolicited 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 ~~e-mail~~ 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 ~~electronic~~ contact details **for electronic message** in accordance with Regulation (EU) 2016/679.

~~(3633a)~~ Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, ~~given that they~~ are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish and or maintain national systems ~~only allowing such calls~~ **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**.

- (34) When end-users **who are natural persons** have provided their consent to receiving ~~unsolicited direct marketing~~ communications ~~for direct marketing purposes~~, 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 ~~unsolicited messages for~~ 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 ~~unsolicited commercial direct marketing~~ communications ~~for direct marketing purposes~~. **Unsolicited Direct** marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person ~~transmitting~~ **sending** the communication **and, where applicable, or on whose behalf of whom** the communication is ~~transmitted sent~~ and provide the necessary information for recipients **end-users who are natural persons** to exercise their right to ~~oppose~~ **withdraw their consent** to receiving further ~~written and/or oral marketing messages~~ **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.**
- (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~~ **present** their identity line on which the company can be called. **Member States are encouraged to introduce by means of national law or present 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.**

- (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.~~
- (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 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. 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.~~

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

- (41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the collection. ~~Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems.~~ It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016⁹. 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.

⁹ Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016 (OJ L 123, 12.5.2016, p. 1–14).

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

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural ~~and legal~~ persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.
 - 1a. **This Regulation lays down rules regarding the protection of the fundamental rights and freedoms of legal persons in the provision and use of the electronic communications services, and in particular their rights to respect of communications.**
2. ~~This Regulation ensures~~ **The** free movement of electronic communications data and electronic communications services within the Union, ~~which~~ shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural ~~and legal~~ persons and the protection of natural persons with regard to the processing of personal data, **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~~ to 2.

Article 2
Material Scope

1. This Regulation applies to:
 - (a) the processing of electronic communications **content data and of electronic communications metadata** carried out in connection with the provision and the use of electronic communications services; ~~and to~~
 - (b) **end-users' terminal equipment** information ~~related to the terminal equipment of end-users.~~
 - (d) **the offering of a publicly available directory of end-users of electronic communications services;**
 - (e) **the sending of direct marketing communications to end-users.**
2. This Regulation does not apply to:
 - (a) activities **which fall outside the scope of Union law, and in any event activities concerning national security and defence;**
 - (b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;

- (c) electronic communications services which are not publicly available;
 - (d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
 - (e) **electronic communications data processed after receipt by the end-user concerned, ~~or by a third party entrusted by that end-user;~~**
 - ~~(f) **electronic communications data processed upon receipt by the end users concerned, or by a third party entrusted by the end-user in order to ensure the security of the end-user's network and information systems including their terminal equipment.**~~
3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) ~~00/0000-2018/1725~~ [new Regulation replacing Regulation 45/2001].
 4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC¹⁰, 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.

¹⁰ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1–16).

Article 3

Territorial scope and representative

1. This Regulation applies to:
 - (a) the provision of electronic communications services to end-users **who are** in the Union,
~~irrespective of whether a payment of the end-user is required;~~
 - (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;~~
 - (c) the protection of **terminal equipment** information ~~related to the terminal equipment~~ of end-users ~~located~~ **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 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 a representative in the Union.

- 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.**
3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located.
4. The representative shall ~~have the power to answer questions and provide information~~ **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.
5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against ~~a natural or legal person who processes electronic communications data in connection with the provision of electronic communications services from outside the Union to end-users in the Union~~ **the provider or person it represents.**

Article 4

Definitions

1. For the purposes of this Regulation, following definitions shall apply:
- (a) the definitions in Regulation (EU) 2016/679;

- (b) the definitions of ‘electronic communications network’, ‘electronic communications service’, ‘interpersonal communications service’, ‘number-based interpersonal communications service’, ‘number-independent interpersonal communications service’, ‘end-user’ and ‘call’ in ~~points~~ **paragraphs** (1), (4), (5), (6), (7), (14) and (21~~31~~) respectively of Article 2 of ~~[Directive (EU) 2018/1972 establishing the European Electronic Communications Code]~~;
- (c) the definition of 'terminal equipment' in ~~point (1)~~ of Article 1(**1**) of Commission Directive 2008/63/EC¹¹;
- (d) **the definition of ‘information society service’ in point (b) of Article 1 (1) of Directive (EU) 2015/1535¹².**

2. For the purposes of ~~point (b) of paragraph 1~~ **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.

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.

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;

¹¹ Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20–26).

¹² Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1-15).

- (b) ‘electronic communications content’ means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;
- (c) ‘electronic communications metadata’ means data processed ~~in an~~ **by means of** electronic communications ~~network~~ **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~~ **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~~ **message**’ 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, **including e-mail, SMS, MMS and functionally equivalent applications and techniques;**
- (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 ~~identified or identifiable~~ **specific** end-users of ~~electronic communications services,~~ including the **placing of voice-to-voice calls,** the use of automated calling and communication systems with or without human interaction, electronic ~~mail message,~~ **SMS,** etc.;

- (g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems;
- (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;
- (i) **'direct marketing calls' means direct marketing voice-to-voice calls and calls made via automated calling and communication systems for the purpose of direct marketing.**

Article 94a

Consent

1. The ~~definition of and conditions~~ **provisions** for consent provided for under ~~Articles 4(11) and 7 of Regulation (EU) 2016/679/EU~~ shall apply **to natural persons and, *mutatis mutandis*, to legal persons.**
- 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.**
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.**
- 2a. **As far as the controller 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).**
3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6**b** ~~(2)~~ and points (a) and (b) of Article 6**a** ~~(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 the possibility to withdraw their consent** at periodic intervals of **no longer than 612 months**, as long as the processing continues, **unless the end-user requests not to receive such reminders.**

CHAPTER II

PROTECTION OF ELECTRONIC COMMUNICATIONS OF ~~NATURAL AND LEGAL PERSONS~~ **END-USERS** AND OF ~~INFORMATION STORED IN~~ **THE INTEGRITY OF THEIR** TERMINAL EQUIPMENT

Article 5

Confidentiality of electronic communications data

Electronic communications data shall be confidential. Any **interference with** electronic communications data, ~~such as by~~ **including** listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance ~~or~~ **and** processing of electronic communications data, by ~~persons~~ **anyone** other than the end-users **concerned**, shall be prohibited, except when permitted by this Regulation.

Article 6

Permitted processing of electronic communications data

1. Providers of electronic communications networks and services ~~may~~ **shall be permitted to** process electronic communications data **only** if:
 - (a) it is necessary to ~~provide an electronic communication service~~ **achieve the transmission of the electronic communication**, ~~for the duration necessary for that purpose~~; or
 - (b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors **and/or security risks and/or attacks** in the transmission of electronic communications, ~~for the duration necessary for that purpose~~;
 - (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 in accordance with Article 11, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security.**

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 6be and if the specified purpose or purposes cannot be fulfilled by processing information that is made anonymous.**
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 6be provided that the conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.**

Article 6a [previous art. 6(3)]

Permitted processing of electronic communications content

31. **Without prejudice to Article (6)(1), Providers of the electronic communications networks and services may shall be permitted to process electronic communications content only:**
 - ~~(a) — for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or~~
 - (a) for the purpose of the provision of an service requested by an end-user for purely individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interests of another person concerned; or**

- (b) 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~~
2. ~~the provider has~~ **Prior to the processing in accordance with point (b) of paragraph 1 the provider shall carry out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data and** consulted the supervisory authority **if necessary pursuant to Article 36(1) of Regulation (EU) 2016/679. Points (2) and (3) of Article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.**

Article 6b [previous art 6(2)]

Permitted processing of electronic communications metadata

- 2.1. **Without prejudice to Article (6)(1), P**providers of electronic communications **networks and services may shall be permitted to process electronic communications metadata only** if:
- (a) ~~it is necessary for the purposes of network management or network optimisation, or to meet mandatory technical quality of service requirements pursuant to [Directive (EU) 2018/1972 establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120¹³ for the duration necessary for that purpose; or~~

¹³ ~~Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).~~

- (b) ~~it is necessary for calculating and billing interconnection payments or for the performance of an electronic communications service contract to which the end-user is party, in particular if necessary for billing, calculating interconnection payments, or if it is necessary for detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or~~
- (c) the end-user concerned has given ~~his or her~~ consent to the processing of ~~his or her~~ communications metadata for one or more specified purposes, ~~including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous; or~~
- (ca) it is necessary for the provision of an electronic communications service for which the end-user has concluded a contract; or
- (d) it is necessary to protect the vital interest of a natural person, in the case of emergency, in general upon request of a public authority, in accordance with Union or Member State law; or
- (e) it is necessary for the purpose of the legitimate interests pursued by the electronic communications service or network provider, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user, in particular where the end-user is a child.

The end-user's interests shall be deemed to override the interests of the electronic communications service or network provider if the provider uses the electronic communications metadata to determine the nature and characteristics of the end-user or to build an individual profile of the end-user. The end-user's interests shall also be deemed to override the interests of the provider if the electronic communications metadata contains special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, unless the conditions set out in Article 9(2)(g) and (j) of Regulation (EU) 2016/679 are met.

~~(f) — it is necessary for statistical purposes, or for scientific research purposes, provided it 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. Processing of electronic communications metadata under this point shall be done in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.~~

2. Electronic communications metadata processed pursuant to paragraph 1(e) shall not be shared by the provider with any third party without prejudice to Article 6(3) unless it has been made anonymous. Prior to processing electronic communications metadata, the provider shall:

- (a) carry out an assessment of the impact of envisaged processing on the confidentiality of communications and the privacy of end-users in accordance with Article 35 of Regulation (EU) 2016/679, which may result in the prior consultation of the supervisory authority in accordance with Article 36(1) to (3) of Regulation (EU) 2016/679;
- (b) inform the end-user of the envisaged processing operations based on paragraph 1(e) and of the end-user's right to object to such processing, at any time, free of charge and in an easy and effective manner; and
- (c) implement appropriate technical and organisational measures, such as pseudonymisation and encryption.

Article 6e

Compatible processing of electronic communications metadata

1. ~~Where the processing for a purpose other than that for which the electronic communications metadata have been collected under 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, inter alia:~~
- ~~(a) any link between the purposes for which the electronic communications metadata have been collected and the purposes of the intended further processing;~~
 - ~~(b) the context in which the electronic communications metadata have been collected, in particular regarding the relationship between end-users concerned and the provider;~~
 - ~~(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 Article 9 or 10 of Regulation (EU) 2016/679;~~
 - ~~(d) the possible consequences of the intended further processing for end-users;~~
 - ~~(e) the existence of appropriate safeguards, such as pseudonymisation and encryption.~~

~~2. — Such processing, if considered compatible, may only take place, provided that:~~

~~(a) — electronic communications metadata is erased or made anonymous as soon as it is no longer needed to fulfil the purpose,~~

~~(b) — the processing is limited to electronic communications metadata that is pseudonymised, and~~

~~(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.~~

~~3. — For the purposes of this Article, the providers of electronic communications networks and services shall:~~

~~(ab) — not share such data with third parties, unless it is made anonymous;~~

~~(bc) — prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data in accordance with Article 35 of Regulation (EU) 2016/679, which may result in the prior and consultation of the supervisory authority in accordance with Article 36(1) to (3) of Regulation (EU) 2016/679; and~~

~~(cd) — inform the end-user of specific processing on the basis of this Article and of the right to object to such processing free of charge, at any time, and in an easy and effective manner. If the end-user objects, the electronic communications metadata shall no longer be processed for such purposes.~~

[Article 6d

Processing of electronic communications data for the purpose of preventing child sexual abuse

1. Without prejudice to Article (6)1, providers of number-independent interpersonal communications services shall be permitted to process electronic communication data for the sole purpose of preventing child sexual abuse and exploitation by detecting, deleting and reporting material as defined in Article 2(c) of Directive 2011/93/EU, if the processing meets all of the following characteristics:

- (i) it creates a unique, non-reconvertible digital signature (“hash”) of material attached to electronic communications for the sole purpose of comparing that hash with a database containing hashes of material previously reliably identified as constituting material defined in Article 2(c) of Directive 2011/93/EU;**
- (ii) electronic communications data and hashes of material attached to electronic communications are erased immediately after comparison with the database, except in the cases where material constituting material defined in Article 2(c) of Directive 2011/93/EU has been detected by virtue of a hash.**

- 2. The provider of number-independent interpersonal communications services shall, prior to processing, carry out an assessment of the impact and consult the supervisory authority, in accordance with Article 35 and 36 of Regulation (EU) 2016/679. The assessment of impact shall include a description of the processing activities concerning both automatic and manual processing of the data, including description of possible algorithms or databases used for the processing and means to limit the rate of erroneous detection of material defined in Article 2(c) of Directive 2011/93/EU and of the security measures, including limitation of personnel authorised to access electronic communications data, set up to protect end-users not involved in the communication of material defined in Article 2(c) of Directive 2011/93/EU, and to protect the consulted content.**
- 3. The provider of number-independent interpersonal communications services shall inform the users about the processing taking place in accordance with this article and provide suitable complaint procedure.]**

Article 7

Storage and erasure of electronic communications data

1. ~~Without prejudice to points (b) of Article 6(1) and points (a), and (b) of Article 6(3),~~ **a, t** 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) after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded, or stored by the end users or by a third party entrusted by them to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679.**
2. Without prejudice to points (b), **(c) and (d)** of Article 6(1), ~~and points (a), (c), (ca), (d) and to (fe) of Article 6(2)~~ **b(1) and Article 6e**, the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.
3. Where the processing of electronic communications metadata takes place for the purpose of billing ~~in accordance with point (b) of Article 6b(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.
4. **Union or Member state law may provide in accordance with Article 11 that the electronic communications metadata is retained, 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 that is longer than the period set out in this Article .**

Article 8

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

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
 - (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
 - (b) the end-user has given his or her consent; or
 - (c) it is necessary for providing an information society service requested by the end-user; or
 - (d) **if it is necessary for web-audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user or by a third party, or by third parties jointly, on behalf of the one or more providers of the information society service provided that conditions laid down in Article 28, or where applicable Article 26, of Regulation (EU) 2016/679 are met; or**
 - ~~(da) — it is necessary to maintain or restore the security of information society services or terminal equipment of the end-user, prevent fraud 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 are not changed in any way,~~
 - ~~—— (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~~

- (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).**
- (g) it is necessary for the purpose of the legitimate interests pursued by a service provider to use processing and storage capabilities of terminal equipment or to collect information from an end-user’s terminal equipment, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user.**

The end-user’s interests shall be deemed to override the interests of the service provider where the end-user is a child or where the service provider processes, stores or collects the information to determine the nature and characteristics of the end-user or to build an individual profile of the end-user or the processing, storage or collection of the information by the service provider contains special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679.

- 1a. Service providers using processing and storage capabilities of the end-user’s terminal equipment or collecting information from the end-user’s terminal equipment pursuant to paragraph 1(g) shall not share the information with any third party other than its processors, acting in accordance with Article 28 of Regulation (EU) 2016/679 *mutatis mutandis*, unless it has been made anonymous. Prior to any use of processing or storage facilities in, or collection of information from the end-user’s terminal equipment, the service provider shall:**
 - (a) carry out an assessment of the impact of the use of the processing and storage capabilities or the collection of information from the end-users’ terminal equipment and of the envisaged processing on the confidentiality of communications and the privacy of end-users in accordance with Article 35 of Regulation (EU) 2016/679, which may result in the prior consultation of the supervisory authority in accordance with Article 36(1) to (3) of Regulation (EU) 2016/679;**
 - (b) inform the end-user of the envisaged processing operations based on paragraph 1(g) and of the end-user’s right to object to such processing, free of charge, at any time, and in an easy and effective manner; and**

- c) **implement appropriate technical and organisational measures, such as pseudonymisation and encryption.**
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 prohibited, except ~~if~~ **on the following grounds:**
- (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing **or maintaining** a connection; or
 - (b) **the end-user has given his or her consent; or**
 - (c) **it is necessary for the purpose of statistical counting 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.**
- ~~(b)~~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) 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.
- 2b. **For the purpose of paragraph 2 points (b) and (c), ~~T~~the collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.**

3. The information to be provided pursuant to ~~point (b) of~~ paragraph 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.
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 257 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.

Article 9

Consent

1. ~~The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.~~
2. ~~Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.~~
3. ~~End users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.~~

Article 10

Information and options for privacy settings to be provided

- ~~1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.~~
- ~~2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.~~
- ~~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.~~

Article 11
Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)~~(a)~~ (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 paragraph 1.**
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.

CHAPTER III

~~NATURAL AND LEGAL PERSONS~~ END-USERS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS

Article 12

Presentation and restriction of calling and connected line identification

1. Where presentation of the calling and connected line identification is offered in accordance with Article ~~[107]~~**115** of the ~~[Directive (EU) 2018/1972 establishing the European Electronic Communication Code]~~, the providers of publicly available number-based interpersonal communications services shall provide the following:
 - (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;
 - (b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;
 - (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;
 - (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**.
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.

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.
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 **and the exceptions set forth in Article 13.**

Article 13

*Exceptions to presentation and restriction of calling and connected line identification **in relation to emergency communications***

1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where ~~a call is~~ **emergency communications are** 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.

- 1a. Regardless whether the called end-user rejects incoming calls where the presentation of the calling line identification has been prevented by the calling end-user, providers of number-based interpersonal communications services shall override this choice, where technically possible, when the calling end-user is an organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.**
- ~~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.~~
- 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 such location data to determine and provide the calling end-user's location to an organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such calls.**

Article 14

~~*Incoming call blocking*~~ ***Unwanted, malicious or nuisance calls***

1. Providers of ~~publicly available~~ 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. ~~and~~
- 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.**
2. **Providers of number-based interpersonal communications services** shall also provide the called end-user with the following possibilities, free of charge:
 - (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
 - (b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.

Article 15

Publicly available directories

1. The providers of ~~publicly available directories~~ **number-based interpersonal communications services** shall obtain the consent of end-users who are natural persons to include their personal data in the directory and, ~~consequently, shall obtain consent from these end-users~~ for inclusion of **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.
- 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.**
2. The providers of a ~~publicly available directory~~ **number-based interpersonal communications services** shall inform end-users who are natural persons whose personal data are in the directory of ~~the available~~ **any** search functions **that is not based on name or number** ~~of in~~ the directory and obtain **the consent of** end-users' ~~consent~~ before enabling such search functions related to their own data.

3. The providers of ~~publicly available directories~~ **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.
- 3a. ~~The providers of~~ **number-based interpersonal communications services** shall give ~~such end-users that are legal persons~~ the means to verify, correct and delete ~~such 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 for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.
- 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 and ~~D~~direct marketing communications

1. Natural or legal persons ~~may~~ **shall be prohibited from using** electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons ~~that unless they~~ have given their consent.
2. **Notwithstanding paragraph 1, W**where a natural or legal person obtains ~~electronic~~ contact details for electronic ~~mail~~ **message** from ~~its customer~~ **end-users who are natural persons**, in the context of the ~~sale~~ **purchase** 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~~ **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 person sends a message to that end-user for the purpose of direct marketing** ~~is sent~~.
- 2a. **Member States may provide by law a set period of time, after the sale of the product or service occurred, within which a natural or legal person may use contact details of the end-user who is a natural person for direct marketing purposes, as provided for in paragraph 2.**
3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall:

- (a) present the ~~identity of a~~ **calling line identification** on which they can be contacted; ~~or~~.
- (b) **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.**
4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.
5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to ~~unsolicited~~ **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~~ 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 of the legal or natural person on behalf of whom the **direct marketing** communication is ~~transmitted sent~~;
 - ~~(c) 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;~~
 - (cd) **clearly and distinctly give the end-users who are natural persons a means to object or to withdraw their consent, free of charge, at any time, and in an easy and effective manner, to receiving further direct marketing communications, and shall provide the necessary information to this end. This means shall also be given at the time of collection of the contact details according to paragraph 2. It shall be as easy to withdraw as to give consent.**
- ~~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.~~

Article 17

Information about detected security risks

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

CHAPTER IV

INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT

Article 18

~~Independent~~ *Supervisory authorities*

- 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.

- ~~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. Chapters VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.~~

- 1ab. The supervisory authorities shall have investigative and corrective powers, including the power to impose administrative fines pursuant to article 23.**
- 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.**
- 2. Where ~~the supervisory authority or authorities referred to in paragraphs 1~~ 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 the [Directive (EU) 2018/1972 Establishing the European Electronic Communications Code] and other relevant authorities.**

Article 19

European Data Protection Board

1. The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have ~~competence~~ **the task to ensure contribute to** the consistent application of **Chapters I, II and III** 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.~~
2. ~~To that end, the Board shall also~~ have the following tasks:
 - (a) advise the Commission on any proposed amendment of this Regulation;
 - (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 **in relation to Chapters I, II and III** and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;
 - (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;**
 - (da) **issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph to assess for different types of electronic communications services the moment in time of receipt of electronic communications content;**

- (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;**
 - (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;**
3. **Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.**
 4. **The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and make them public.**
 5. **The Board shall consult the supervisory authorities referred to in Article 18(0) before excercising any of the tasks referred to in paragraph 2 where those authorities are not the authorities responsible for monitoring the application of Regulation (EU) 2016/679.**
 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.**

Article 20

Cross-border cooperation ~~and consistency procedures~~

Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union **and cooperate with each other and with the Commission.**

~~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.~~

CHAPTER V

REMEDIES, LIABILITY AND PENALTIES

Article 21

Remedies

1. Without prejudice to any other administrative or judicial remedy, every end-user of ~~electronic communications services~~ shall have the ~~same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679~~ **right to an effective judicial remedy in relation to any infringement of his or her rights under this Regulation, the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy against any decision of a supervisory authority.**

Articles 77-80 of Regulation (EU) 2016/679 shall apply *mutatis mutandis*.

2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation ~~and having a legitimate interest in the cessation or prohibition of alleged infringements~~, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.

Article 22

Right to compensation and liability

Any ~~end-user~~ **person** ~~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.

Article 23

General conditions for imposing administrative fines

1. ~~For the purpose of this Article,~~ **Article 83** ~~Chapter VIII~~ of Regulation (EU) 2016/679 shall apply *mutatis mutandis* to infringements of this Regulation.
2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;
 - ~~(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;~~
 - (c) the obligations of the providers of publicly available directories pursuant to Article 15;
 - (d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.

3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, **and 14**, ~~and 17~~.
5. Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.
7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.
8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.

Article 24

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.
2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than 18 months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.

CHAPTER VI

DELEGATED ACTS AND IMPLEMENTING ACTS

Article 25

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the date of entering into force of this Regulation].
3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

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

Article 26
Committee

1. The Commission shall be assisted by the Communications Committee established under Article ~~44~~**118** of the ~~[Directive (EU) 2018/1972 establishing the European Electronic Communications Code]~~. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011¹⁴.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

¹⁴ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13–18).

CHAPTER VII

FINAL PROVISIONS

Article 27

Repeal

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

Article 28

Monitoring and evaluation clause

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

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

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 Without prejudice to paragraph 3, it~~ This Regulation shall apply from ~~[25 May 2018 one year~~ **24 months from the date of entry into force of this Regulation]** .

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President
